

جامعة ميدأوشن



كلية الإدارة

ماجستير إدارة الأعمال

أثر الأمن السيبراني على ثقة العملاء في المعاملات البنكية الإلكترونية

دراسة ميدانية على المصارف السعودية

إعداد الطالب/

دلال ضويحي القحطاني

إشراف/

د. الفيصّل عبد الحميد محمد حسن

د.فايز جرّاد

العام الدراسي:

2026 – 1447



إِهْدَاء

وَوَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ

بكل فخر واعتزاز اهدي هذا النجاح لنفسي أولاً ثم لكل من سعى معي لإتمام هذه

المسيرة

اهدي تخرجي إلى من دعمني بلا حدود واعطائي بلا مقابل إلى من علمني ان الدنيا
كفاح وسلاحها العلم والمعرفة وإلى من غرس في روحي مكارم الأخلاق داعمي الاول في
مسيرتي وقوتي بعد الله " والدي الغالي "

إلى من جعل الجنة تحت اقدامها إلى من سهلت لي الشدائد بدعائها قدوتي ومعلمتي
الاولى وصديقة أيامي (والدتي الحبيبة)

إلى رفيق الدرب وشريك الحياة الذي كان ومازال داعماً لي في كل خطوة اهدي هذا
النجاح " لزوجي العزيز " الذي أعطاني القوة والإصرار لأواصل هذه المسيرة

والى من شد الله بهم عضدي فكانوا لي خير معين " اخواتي "

إلى قرة عيني ونبض قلبي وأول فرحة لي " ابني فيصل "

شكر وتقدير

ليس بعد التمام أجمل من الحمد، فالحمد لله والشكر له كما ينبغي لجلال وجهه وعظيم سلطانه وكما ينبغي لجزيل فضله وعظيم إحسانه على ما أنعم به على من إتمام هذا البحث.

ثم أنه لا يسعني الا أن أشيد بالفضل وأقر بالمعروف لكل من ساهم في إنجاز هذا البحث.

كل الشكر للجهات التي دعمتني وساعدتني وخصتني بالتوجيه والتصويب لإتمام بحثي على الوجه الصحيح.

كما أتقدم بالشكر لمن كان لتوجيهاتهم الدور الكبير في انجاز هذا المشروع وكل من مد لي يد العون من قريب وبعيد ولو بدعوة بظهر الغيب، بارك الله فيهم جميعاً وجزاهم الله عني الجزاء الأوفى وأسأل الله أن ينفع بهذا البحث على قدر العناء فيه وأن يجعله خالصاً لوجهه الكريم إنه على ذلك لقادر.

المستخلص

تهدف هذه الدراسة إلى التعرف على أثر الأمن السيبراني بأبعاده الأربعة — سرية المعلومات، وسلامة النظام، والموثوقية، والخصوصية — على ثقة العملاء في المعاملات البنكية الإلكترونية، وذلك بالتطبيق على المصارف السعودية. واعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبانة أداة رئيسية لجمع البيانات، حيث وُزعت على عينة عشوائية ميسرة بلغت 450 مفردة من عملاء الخدمات البنكية الإلكترونية، واسترُدت 424 استبانة صالحة للتحليل بمعدل استجابة بلغ 94.2%. وقد عولجت البيانات إحصائياً باستخدام برنامج SPSS ، وطُبقت أساليب تحليلية شملت المتوسطات الحسابية، والانحرافات المعيارية، ومعامل ارتباط بيرسون، ومعامل ألفا كرونباخ، وتحليل الانحدار الخطي البسيط والمتعدد. وتوصلت الدراسة إلى وجود أثر إيجابي ذي دلالة إحصائية عند مستوى $(\alpha \leq 0.01)$ لأبعاد الأمن السيبراني مجتمعةً على ثقة العملاء، بمعامل تحديد بلغ $(R^2 = 0.709)$ كما أثبتت النتائج أن الموثوقية هي البعد الأكثر تأثيراً، تليها سرية المعلومات، ثم الخصوصية، وأخيراً سلامة النظام. وأوصت الدراسة بتعزيز البنية التحتية لموثوقية الأنظمة المصرفية الإلكترونية، وتبني سياسات خصوصية أكثر شفافية، وتكثيف برامج التوعية الأمنية الموجهة للعملاء.

الكلمات المفتاحية: الأمن السيبراني، سرية المعلومات، سلامة النظام، الموثوقية، الخصوصية، ثقة العملاء، المعاملات البنكية الإلكترونية، المصارف السعودية.

قائمة المحتويات

أ.....	بسم الله الرحمن الرحيم
ب.....	الإهداء
ج.....	الشكر والتقدير
د.....	المستخلص
ه.....	قائمة المحتويات
ح.....	قائمة الجداول
1.....	الفصل الأول: الإطار العام للدراسة
1.....	1.1 المقدمة
2.....	2.1 مشكلة الدراسة
3.....	3.1 أهمية الدراسة
5.....	4.1 أهداف الدراسة
5.....	5.1 تساؤلات الدراسة
6.....	6.1 فروض الدراسة
6.....	7.1 الدراسات السابقة
18.....	8.1 الفجوة البحثية
19.....	9.1 المنطلقات النظرية للدراسة
22.....	10.1 المنهجية وطرق البحث
25.....	11.1 الأساليب الإحصائية المستخدمة
26.....	12.1 حدود الدراسة
27.....	الفصل الثاني: الإطار النظري
27.....	المبحث الأول: الأمن السيبراني (المتغير المستقل)
27.....	1.1.2 تمهيد
27.....	2.1.2 مفهوم الأمن السيبراني

3.1.2 أهمية الأمن السيبراني في القطاع المصرفي.....	29
4.1.2 أهداف الأمن السيبراني في القطاع المصرفي.....	30
5.1.2 أبعاد الأمن السيبراني.....	32
6.1.2 استراتيجيات الأمن السيبراني في القطاع المصرفي.....	36
7.1.2 التحديات المعاصرة للأمن السيبراني المصرفي.....	37
المبحث الثاني: ثقة العملاء في المعاملات البنكية الإلكترونية.....	39
1.2.2 تمهيد.....	39
2.2.2 مفهوم ثقة العملاء.....	39
3.2.2 أهمية ثقة العملاء في الخدمات المصرفية الإلكترونية.....	41
4.2.2 أهداف بناء ثقة العملاء في البيئة المصرفية الرقمية.....	42
5.2.2 محددات ثقة العملاء في المعاملات البنكية الإلكترونية.....	43
6.2.2 استراتيجيات بناء وتعزيز ثقة العملاء.....	44
7.2.2 العلاقة النظرية بين الأمن السيبراني وثقة العملاء.....	45
الفصل الثالث: منهجية الدراسة.....	47
1.3 تمهيد.....	47
2.3 منهج الدراسة.....	47
3.3 مجتمع الدراسة وعينتها.....	47
4.3 أداة الدراسة (الاستبانة).....	49
5.3 صدق أداة الدراسة.....	50
6.3 ثبات أداة الدراسة.....	51
7.3 الأساليب الإحصائية المستخدمة.....	52
الفصل الرابع: تحليل البيانات واختبار الفرضيات.....	54
1.4 تحليل البيانات الديموغرافية لأفراد العينة.....	54
2.4 التحليل الوصفي لمجاور الدراسة وأبعادها.....	57
3.4 فرضيات الدراسة.....	64

71.....	الفصل الخامس: النتائج والتوصيات
71.....	1.5 نتائج الدراسة
74.....	2.5 التوصيات
76.....	Abstract
77.....	المراجع
77.....	المراجع العربية
81.....	المراجع الأجنبية
83.....	الملاحق
84.....	استمارة استبيان

قائمة الجداول

رقم الصفحة	اسم الجدول	رقم الجدول
48	جدول (1) توزيع الاستبانات ومعدل الاستجابة	1.
49	جدول (2): توزيع فقرات الاستبانة على محاور الدراسة	2.
51	جدول (3): مصفوفة معاملات الارتباط بين متغيرات الدراسة	3.
51	جدول (4): معاملات ثبات ألفا كرونباخ لأبعاد الدراسة	4.
54	جدول (5): توزيع أفراد العينة وفقاً للنوع	5.
54	جدول (6): توزيع أفراد العينة وفقاً للفئة العمرية	6.
55	جدول (7): توزيع أفراد العينة وفقاً للمؤهل العلمي	7.
55	جدول (8): توزيع أفراد العينة وفقاً لمدة استخدام الخدمات المصرفية الإلكترونية	8.
56	جدول (9): توزيع أفراد العينة وفقاً لمعدل تكرار الاستخدام	9.
57	جدول (10): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد سرية المعلومات	10.
58	جدول (11): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد سلامة النظام	11.

رقم الصفحة	اسم الجدول	رقم الجدول
59	جدول (12): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الموثوقية	12.
60	جدول (13): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الخصوصية	13.
61	جدول (14): ترتيب أبعاد الأمن السيبراني وفقاً للمتوسطات الحسابية	14.
62	جدول (15): المتوسطات الحسابية والانحرافات المعيارية لفقرات محور ثقة العملاء	15.
65	جدول (16): نتائج تحليل الانحدار المتعدد لأثر أبعاد الأمن السيبراني على ثقة العملاء	16.
66	جدول (17): تحليل الانحدار الخطي البسيط لقياس أثر سرية المعلومات على ثقة العملاء	17.
67	جدول (18): تحليل الانحدار الخطي البسيط لقياس أثر سلامة النظام على ثقة العملاء	18.
69	جدول (19): تحليل الانحدار الخطي البسيط لقياس أثر الموثوقية على ثقة العملاء	19.
70	جدول (20): تحليل الانحدار الخطي البسيط لقياس أثر الخصوصية على ثقة العملاء	20.

الفصل الأول: الإطار العام للدراسة

1.1 المقدمة

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 يساهم 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.

2.1 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 يسهم 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 بالملكة 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؟

3.1 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.
- ترفد 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

- تمكن 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.

4.1 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.

5.1 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 المعاملات 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؟

6.1 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 المعاملات 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.

7.1 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 الرئيسة 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 يساهم 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 (البدوى، 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 (لحمر، 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 لتقوية العلاقة مع العملاء وتحسين تجربتهم المصرفية الإلكترونية

□ دراسة (فؤاد وعراقات، 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 الإلكتروني. 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 لتقوية 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 وتبنّيها 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.

8.1 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، تنبع 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.

9.1 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 متكاملاً 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 مكملًا 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: المصداقية، 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 تُكسب 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.

ختامًا، يمكن القول إن الأمن السيبراني لم يعد مجرد أداة تقنية لحماية الأنظمة البنكية، بل أصبح عنصرًا استراتيجيًا 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، استنادًا إلى الأدلة النظرية والتطبيقية الحديثة في المجال (الشمري، 2020؛ Safa et al., 2019؛ Alharthi, 2022؛ Alqahtani & Kavakli, 2021).

10.1 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).

مجتمع الدراسة

سيتمكّن مجتمع الدراسة من جميع عملاء المصارف السعودية الذين سيستخدمون الخدمات البنكية الإلكترونية عبر المواقع الرسمية أو تطبيقات الهاتف المحمول. ووفقًا 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 نظرًا لارتباطه المباشر بموضوع الأمن السيبراني والثقة في المعاملات البنكية الإلكترونية، إذ سيُعد العملاء المستخدمون فعليًا للخدمات الرقمية الفئة الأكثر تأثرًا بمستوى الحماية الإلكترونية وفعالية الإجراءات الأمنية المتبعة في المصارف السعودية.

عينة الدراسة

سيتم اختيار عينة عشوائية بسيطة من عملاء المصارف السعودية بهدف تمثيل المجتمع تمثيلًا علميًا دقيقًا. ومن المتوقع أن يبلغ حجم العينة 176 مفردة، وهو حجم مناسب من الناحية الإحصائية وفقًا لمعادلة Krejcie & Morgan (1970) لتحديد العينات من المجتمعات الكبيرة، مما يضمن مستوى ثقة يبلغ 95% وهامش خطأ $\pm 5\%$. وسيتم توزيع الاستبانات إلكترونيًا 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..

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 استنادًا إلى الإطارين النظري والميداني، وإلى ما ورد في الدراسات السابقة ذات الصلة بموضوع الأمن السيبراني والثقة الرقمية في البيئة المصرفية. وستكون 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 سيقسم 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.

وسيتم عرض الاستبانة على مجموعة من المحكمين الأكاديميين والمتخصصين في مجالي الإدارة والمصارف للتأكد من صدقها الظاهري ومناسبتها لأهداف الدراسة. وبعد اعتمادها، ستجرى 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.

11.1 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 بآثر 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.

12.1 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:** ستُجرى الدراسة ميدانيًا 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 فعليًا للخدمات البنكية الإلكترونية.

الفصل الثاني: الإطار النظري

المبحث الأول: الأمن السيبراني (المتغير المستقل)

1.1.2 تمهيد

شهد القطاع المصرفي تحولات جوهرية في بنيته التشغيلية خلال العقدَيْن الأخيرَيْن، إذ انتقلت المعاملات المالية من الفروع التقليدية إلى منصات رقمية مفتوحة تعمل على مدار الساعة وتتيح للعملاء إجراء عملياتهم من أي مكان في العالم. وقد أفرز هذا التحول الرقمي المتسارع تحديات أمنية غير مسبوقة، حيث أصبحت البنوك هدفًا رئيسيًا للهجمات السيبرانية نظرًا لحجم البيانات المالية الحساسة التي تحتفظ بها وطبيعة العمليات التي تجريها. وفي هذا السياق، لم يعد الأمن السيبراني مجرد وظيفة تقنية هامشية، بل تحول إلى ضرورة استراتيجية تمس صميم استمرارية المؤسسة المصرفية وقدرتها التنافسية وعلاقتها بعملائها. ويتناول هذا المبحث مفهوم الأمن السيبراني وتعريفاته في الأدبيات الأكاديمية والمهنية، ثم ينتقل إلى أهميته في القطاع المصرفي وأهدافه وأبعاده التي اعتمدتها الدراسة الحالية، فضلاً عن الاستراتيجيات المطبقة لتحقيقه والتحديات التي تواجه تطبيقه في البيئة المصرفية السعودية.

2.1.2 مفهوم الأمن السيبراني

يُعد مفهوم الأمن السيبراني من المفاهيم التي تطورت بشكل متسارع بفعل التغيرات التقنية والتهديدات المتجددة، وقد تعددت تعريفاته في الأدبيات الأكاديمية والمهنية تبعًا للزاوية التي ينظر منها كل باحث أو مؤسسة إلى هذا المفهوم. فمن المنظور التقني، عرّفه الهلسه والشيخ (2021) بأنه مجموعة من الأدوات والتقنيات والإجراءات التي تهدف إلى حماية الأنظمة الحاسوبية والشبكات والبيانات من أي وصول غير مصرّح به أو تعديل أو إتلاف، مع التركيز على الجوانب التقنية المتصلة بالتشفير وأنظمة كشف التسلل والجدران النارية. وقد ركز هذا التعريف على البُعد الوقائي للأمن السيبراني بوصفه خط الدفاع الأول في مواجهة التهديدات الإلكترونية.

ومن زاوية إدارية أوسع، نظرت حسين وأبو الغنم (2022) إلى الأمن السيبراني باعتباره منظومة متكاملة تشمل السياسات والإجراءات والهياكل التنظيمية التي تضعها المؤسسة لحماية أصولها المعلوماتية وسمعتها المؤسسية، وهو ما يتجاوز البُعد التقني المحض ليشمل الحوكمة وإدارة المخاطر والامتثال التنظيمي. ويُبرز هذا التعريف أن الأمن السيبراني ليس مسؤولية قسم تقنية المعلومات وحده، بل هو مسؤولية مؤسسية شاملة تتطلب تضافر جميع المستويات الإدارية.

وفي السياق المصرفي تحديداً، عرّفه زريقات والحوامده (2022) بأنه الإطار الحوكمي والتقني الذي تتبناه المؤسسات المالية لضمان سرية المعلومات وسلامة الأنظمة وموثوقية العمليات وخصوصية بيانات العملاء في بيئة التجارة الإلكترونية، مشيراً إلى أن هذا الإطار يجب أن يتوافق مع المعايير الدولية والتنظيمات المحلية المعمول بها. أما العبدالله والشورة (2023) فقد عرّفاه من منظور تسويقي بوصفه القدرة التنظيمية التي تمكّن البنك من حماية قنواته الرقمية وبيانات عملائه بما يضمن استمرارية العلاقة التسويقية وتعزيز ثقة العملاء في التعاملات الإلكترونية.

وعلى المستوى المؤسسي الرسمي، عرّفت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية الأمن السيبراني بأنه حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. كما عرّفه البنك المركزي السعودي بأنه مجموعة من الأدوات والسياسات والمفاهيم الأمنية وتدابير الوقاية الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريبات وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية أصول معلومات المؤسسات المالية ضد التهديدات الداخلية والخارجية.

ومن جهته، تناول عبد الفاتح (2022) المفهوم من بُعد وعي العملاء، حيث نظر إلى الأمن السيبراني بوصفه حالة الحماية التي يدركها العميل ويُقيّمها بناءً على معارفه ومهاراته وخبراته في التعامل مع البيئة الرقمية المصرفية، مما يعني أن الأمن السيبراني لا يقتصر على ما تطبقه المؤسسة فعلياً، بل يمتد ليشمل تصور العميل لمستوى هذه الحماية. أما البوانه وصالح (2023) فقد تناولوا المفهوم من زاوية المخاطر،

وعرفاه بأنه القدرة على تحديد التهديدات السيبرانية وتقييمها والاستجابة لها بما يحمي الأصول المعلوماتية والمالية للمؤسسة وعملائها.

وفي ضوء هذه التعريفات المتنوعة، يرى الباحث أن الأمن السيبراني في السياق المصرفي يمكن تعريفه بأنه منظومة متكاملة من السياسات التنظيمية والأدوات التقنية والممارسات الإدارية والأطر القانونية التي يتبناها البنك لحماية بنيته التحتية الرقمية وبيانات عملائه ومعاملاتهم المالية من التهديدات السيبرانية بأشكالها كافة، بما يضمن سرية المعلومات وسلامة الأنظمة وموثوقية الخدمات وخصوصية البيانات، ويُعزز في الوقت ذاته ثقة العملاء واستمرارية العمليات المصرفية. ويتميز هذا التعريف بشموليته للأبعاد التقنية والإدارية والقانونية والإنسانية، فضلاً عن ربطه بين الأمن السيبراني كمتغير مستقل وثقة العملاء كمتغير تابع وهو ما تسعى الدراسة الحالية إلى اختباره.

3.1.2 أهمية الأمن السيبراني في القطاع المصرفي

تزايد أهمية الأمن السيبراني في القطاع المصرفي بشكل مطّرد مع تعمّق التحول الرقمي وتوسّع نطاق الخدمات المالية الإلكترونية، إذ أصبحت البنوك تعتمد اعتماداً شبيه كلي على البنية التحتية الرقمية في إدارة عملياتها اليومية وخدمة عملائها. ولم تعد أهمية هذا المفهوم محصورة في الجانب التقني فحسب، بل امتدت لتشمل أبعاداً استراتيجية واقتصادية وتنظيمية وسمعية تمس جوهر عمل المؤسسة المصرفية.

وتشير دراسة حسين وأبو الغنم (2022) إلى أن أهمية الأمن السيبراني في البنوك تتجلى في عدة محاور رئيسية: 1- حماية سمعة البنك ومكانته التنافسية، إذ يؤدي أي اختراق أمني إلى تآكل ثقة العملاء والمساهمين والجهات الرقابية في المؤسسة، وقد يترتب عليه خسائر مالية فادحة تتجاوز تكلفة الاختراق المباشر لتشمل فقدان العملاء وتراجع الحصة السوقية. 2- ضمان استمرارية العمليات المصرفية، حيث إن أي تعطل في الأنظمة الإلكترونية نتيجة هجوم سيبراني يُلحق ضرراً مباشراً بقدرة البنك على خدمة عملائه وتنفيذ التزاماته المالية. 3- الامتثال للمتطلبات التنظيمية والرقابية التي تفرضها الجهات المختصة، والتي أصبحت تتضمن معايير صارمة للأمن السيبراني في المؤسسات المالية.

ويرى الهلسه والشيخ (2021) أن أهمية الأمن السيبراني في البنوك تتمثل في كونه: 1- ضامناً لجودة المخرجات المحاسبية والمالية، حيث إن أي تلاعب في البيانات نتيجة اختراق سيبراني يُفقد التقارير المالية مصداقيتها ويُعرض البنك لمخاطر قانونية وتنظيمية جسيمة 2- عاملاً محورياً في دعم عمليات اتخاذ القرار، إذ تعتمد الإدارة العليا على بيانات دقيقة وموثوقة في رسم السياسات والاستراتيجيات. 3- ركيزة أساسية لتفعيل آليات الحوكمة والرقابة الداخلية، حيث تتطلب الحوكمة الفعالة وجود نظم معلومات آمنة وموثوقة تكفل الشفافية والمساءلة.

كما يؤكد زريقات والحوامده (2022) أن أهمية الأمن السيبراني تبرز بقوة في مجال التجارة الإلكترونية المصرفية، إذ يُعد شرطاً لازماً لفعالية المعاملات الإلكترونية العابرة للحدود، ولا يمكن للبنوك الانخراط في التجارة الإلكترونية العالمية دون توفير مستوى عالٍ من الحماية السيبرانية يتوافق مع المعايير الدولية. وتُضيف دراسة العبدلات والشورة (2023) بُعداً تسويقياً لهذه الأهمية، حيث أوضحت أن الأمن السيبراني يُشكّل عنصراً جوهرياً في المزيج التسويقي الإلكتروني للبنوك، وأن العملاء يضعونه في مقدمة العوامل التي يقيمون على أساسها جودة الخدمة المصرفية الرقمية.

وفي السياق السعودي تحديداً، تبرز أهمية الأمن السيبراني بشكل خاص في ظل رؤية المملكة 2030 التي تسعى إلى بناء اقتصاد رقمي متقدم، حيث يُعد القطاع المصرفي من أبرز القطاعات المستهدفة بالتحول الرقمي. وقد أكدت دراسة الغامدي والمصطفي (2021) أن الأمن السيبراني يُسهم في تحقيق الميزة التنافسية للمؤسسات الوطنية، مما يجعله أداة استراتيجية لتعزيز مكانة القطاع المصرفي السعودي على المستويين الإقليمي والدولي.

4.1.2 أهداف الأمن السيبراني في القطاع المصرفي

تتعدد أهداف الأمن السيبراني في القطاع المصرفي وتنشعب بتنشعب المخاطر والتهديدات التي يواجهها هذا القطاع الحيوي. وقد تناول الباحثون هذه الأهداف من زوايا مختلفة تعكس تنوع اهتماماتهم البحثية وتخصصاتهم الأكاديمية.

فمن المنظور المحاسبي والمالي، حدد الهلسه والشيخ (2021) ثلاثة أهداف رئيسية

- حماية سلامة المعلومات المحاسبية وضمان دقتها واكتمالها بما يُمكن أصحاب المصلحة من اتخاذ قرارات مبنية على بيانات موثوقة
- تعزيز خصائص الإفصاح المالي من حيث الملاءمة والموثوقية والقابلية للمقارنة، وهي خصائص لا يمكن تحقيقها دون بيئة معلوماتية آمنة
- دعم أطر الحوكمة المؤسسية من خلال توفير نظم رقابية فعالة تحول دون التلاعب بالبيانات أو الوصول غير المشروع إليها.

ومن المنظور الاستراتيجي والتنافسي، أشارت دراسة الغامدي والمصطفي (2021) إلى أهداف تتمثل في :

- تحقيق الميزة التنافسية المستدامة من خلال بناء بنية أمنية متقدمة تُميّز المؤسسة عن منافسيها .
- دعم الأمن الوطني بوصف القطاع المصرفي جزءاً من البنية التحتية الحرجة للدولة .
- تعزيز قدرة المؤسسة على الابتكار الرقمي في بيئة آمنة تشجع على تقديم خدمات جديدة دون تعريض الأصول المعلوماتية للخطر.

أما من منظور حوكمة الأمن السيبراني، فقد حدد زريقات والحوامده (2022) مجموعة من الأهداف تشمل

- إرساء إطار حوكمي واضح يحدد الأدوار والمسؤوليات ويضمن المساءلة على جميع المستويات الإدارية .
 - تطوير قدرات الاستجابة للحوادث الأمنية وتقليل زمن التعافي منها .
 - تحقيق التوافق بين متطلبات الأمن السيبراني وأهداف الأعمال الاستراتيجية للبنك .
- وأضاف عبد الفاتح (2022) أهدافاً مرتبطة بالبُعد الإنساني والتوعوي تتمثل في :
- رفع مستوى الوعي الأمني لدى العملاء وتمكينهم من حماية أنفسهم في البيئة الرقمية .

- تطوير المعارف والمهارات الأمنية لدى الموظفين بما يجعلهم خط دفاع فعالاً.
- بناء ثقافة أمنية مؤسسية تجعل الأمن السيبراني جزءاً من الممارسات اليومية وليس مجرد إجراءات شكلية.

5.1.2 أبعاد الأمن السيبراني

تم تحديد أبعاد الأمن السيبراني المعتمدة في هذه الدراسة بناءً على مراجعة شاملة للأدبيات ذات الصلة، ولا سيما دراسة الهلسه والشيخ (2021) التي تناولت مقومات الأمن السيبراني في البنوك التجارية، ودراسة الغامدي والمصطفي (2021) التي فحصت أبعاد الأمن السيبراني وأثرها على الميزة التنافسية، ودراسة زريقات والحوامده (2022) التي عالجت حوكمة الأمن السيبراني في البيئة المصرفية، فضلاً عن نموذج الثلاث الأمني (CIA Triad) الذي يُعد الإطار المرجعي الأكثر شيوعاً في أدبيات أمن المعلومات. وقد استقر الباحث على أربعة أبعاد هي: سرية المعلومات، وسلامة النظام، والموثوقية، والخصوصية، وذلك لكونها تعكس الجوانب الأكثر ارتباطاً بتجربة العميل المصرفي الإلكتروني وأكثرها قابلية للقياس من منظور إدراك العملاء.

البُعد الأول: سرية المعلومات

تُشير سرية المعلومات إلى ضمان عدم وصول البيانات والمعلومات إلا للأشخاص المخولين بذلك، وهي من أقدم المبادئ الأمنية وأكثرها رسوخاً في الممارسة المصرفية. وتكتسب السرية أهمية استثنائية في البيئة المصرفية نظراً لطبيعة البيانات التي تتعامل معها البنوك، والتي تشمل أرصدة الحسابات وتفاصيل التحويلات والبيانات الشخصية للعملاء والمعلومات الائتمانية، وهي بيانات يمكن أن يترتب على كشفها أضرار مالية ومعنوية جسيمة للعملاء والمؤسسة على حد سواء.

وتتحقق السرية في البيئة المصرفية الإلكترونية من خلال منظومة متكاملة من الآليات التقنية والإدارية. فعلى الصعيد التقني، تعتمد البنوك على بروتوكولات التشفير المتقدمة مثل معيار التشفير المتقدم (AES-256) وبروتوكول الطبقة الأمانة (TLS/SSL) لتأمين البيانات أثناء نقلها وتخزينها. كما تُطبّق

آليات المصادقة متعددة العوامل (MFA) التي تتطلب من المستخدم تأكيد هويته عبر أكثر من وسيلة قبل السماح له بالوصول إلى حسابه. وعلى الصعيد الإداري، تضع البنوك سياسات تحكم الوصول قائمة على مبدأ الحد الأدنى من الصلاحيات (Least Privilege) ونظام التحكم في الوصول القائم على الأدوار (RBAC)، بحيث لا يصل كل موظف إلا إلى البيانات التي يحتاجها لأداء مهامه المحددة.

وقد أكدت دراسة الغامدي والمصطفي (2021) أن السرية تمثل البُعد الأقوى تأثيراً في تعزيز الميزة التنافسية للمؤسسات، وهو ما يعكس الأهمية التي يوليها المتعاملون لهذا البُعد عند تقييمهم لمستوى الأمان. كما أوضحت دراسة العبد اللات والشورة (2023) أن إدراك العملاء لمستوى سرية بياناتهم يُعد مدخلاً أساسياً لبناء العلاقة التسويقية في بيئة الخدمات المصرفية الإلكترونية. ومن جهته، بين عبد الفاتح (2022) أن وعي العملاء بإجراءات السرية المتبعة في البنوك يرتبط ارتباطاً مباشراً بمستوى ثقتهم في التعاملات الإلكترونية.

البُعد الثاني: سلامة النظام

تعني سلامة النظام ضمان دقة البيانات واتساقها واكتمالها وعدم تعرضها لأي تعديل غير مصرح به طوال دورة حياتها، من لحظة إنشائها مروراً بمعالجتها ونقلها وتخزينها. وفي السياق المصرفي، تتجسد سلامة النظام في ضمان أن كل عملية مالية يُجريها العميل — سواء كانت تحويلاً أو دفعة أو استعلاماً — تنعكس بدقة تامة في سجلات البنك دون أي تحريف أو نقصان أو إضافة.

وتعتمد البنوك في تحقيق سلامة النظام على عدة آليات تقنية، من أبرزها دوال التجزئة (Hash Functions) التي تولّد بصمة رقمية فريدة لكل مجموعة بيانات بحيث يمكن كشف أي تغيير مهما كان طفيفاً. كما تُستخدم التوقيعات الرقمية (Digital Signatures) للتحقق من هوية مُرسل البيانات وعدم تعديلها أثناء النقل. وتُضاف إلى ذلك أنظمة كشف التسلل (IDS) التي ترصد أي محاولة للتلاعب بالبيانات أو الأنظمة وتُطلق إنذاراً فورياً. وعلى المستوى الإداري، تُطبّق البنوك سياسات إدارة التغيير التي تضمن أن أي تعديل على الأنظمة أو البيانات يخضع لإجراءات موافقة وتوثيق صارمة، فضلاً عن مسارات التدقيق (Audit Trails) التي تسجل كل عملية وصول أو تعديل مع بيانات المستخدم والتوقيت.

وقد أوضحت دراسة الهلسه والشيخ (2021) أن سلامة نظم المعلومات تُشكّل ركيزة أساسية لجودة المخرجات المحاسبية في البنوك التجارية، إذ لا يمكن الاعتماد على تقارير مالية صادرة عن أنظمة مُعرّضة للتلاعب. كما بيّنت دراسة البوانه وصالح (2023) أن المخاطر المتعلقة بسلامة البيانات تُعد من أبرز العوامل التي تثبط استخدام العملاء للبطاقات المصرفية في البنوك الإسلامية، حيث يخشى العميل من تسجيل عمليات لم يقيم بها أو تحريف مبالغ المعاملات. وأكدت دراسة (Amer and Al-Omar (2023 أن سلامة البيانات تُمثل شرطاً لازماً لنجاح التحول الرقمي في بيئة الأعمال المحاسبية، لكونها تضمن موثوقية المعلومات التي تعتمد عليها عمليات اتخاذ القرار.

البُعد الثالث: الموثوقية

تُعبّر الموثوقية عن قدرة النظام المصرفي الإلكتروني على أداء وظائفه المحددة بشكل صحيح ومنتسق خلال فترة زمنية معينة وتحت ظروف تشغيلية متنوعة، دون أعطال أو توقفات تؤثر على تجربة المستخدم أو سير العمليات المالية. وتتجاوز الموثوقية في مفهومها مجرد التوافر الفني للنظام، لتشمل قدرته على التعامل مع الأحمال المتزايدة ومقاومة الأعطال والتعافي السريع من أي خلل طارئ.

وتتحقق الموثوقية في البيئة المصرفية من خلال عدة مقومات تقنية وتنظيمية. فمن الناحية التقنية، تعتمد البنوك على أنظمة التكرار (Redundancy) التي تتضمن نسخاً احتياطية من الخوادم وقواعد البيانات والشبكات بحيث يستمر النظام في العمل حتى في حالة تعطل أحد مكوناته. كما تُطبّق خطط استمرارية الأعمال (BCP) وخطط التعافي من الكوارث (DRP) التي تحدد الإجراءات الواجب اتباعها لاستعادة الخدمات في أقصر وقت ممكن. وتُجرى اختبارات الأداء والإجهاد (Stress Testing) بشكل دوري للتأكد من قدرة الأنظمة على استيعاب الذروات في حركة التعاملات.

وتكتسب الموثوقية أهمية خاصة في السياق المصرفي السعودي، حيث يشهد القطاع نمواً متسارعاً في أعداد مستخدمي الخدمات المصرفية الإلكترونية، مما يفرض ضغطاً متزايداً على الأنظمة ويجعل أي توقف — مهما كان قصيراً — مؤثراً في أعداد كبيرة من العملاء. وقد أكدت دراسة (Krishna et al. (2025 أن الموثوقية التقنية تُشكّل العمود الفقري لثقة العملاء في الخدمات الرقمية، حيث يربط العملاء بشكل

تلقائي بين استقرار النظام وقدرة المؤسسة على حماية أموالهم ومعلوماتهم. كما أوضحت دراسة زريقات والحوامده (2022) أن حوكمة الأمن السيبراني تعتمد في جوهرها على ضمان استقرار الأنظمة واستمراريتها كمتطلب أساسي لفعالية العمليات المصرفية الإلكترونية. وأشارت دراسة (Amer and Al-Omar (2023 إلى أن استمرارية عمل الأنظمة المحاسبية الرقمية تُعد مؤشراً حاسماً على نضج البيئة الرقمية للمؤسسة وقدرتها على المنافسة.

البُعد الرابع: الخصوصية

تُشير الخصوصية إلى حق الأفراد في التحكم في بياناتهم الشخصية وتحديد كيفية جمعها وتخزينها ومعالجتها ومشاركتها مع أطراف أخرى. وتختلف الخصوصية عن السرية في أن الأخيرة تركز على حماية البيانات من الوصول غير المصرح به بشكل عام، بينما تهتم الخصوصية بالحقوق الفردية للتعامل في تقرير مصير بياناته الشخصية حتى في إطار العلاقة التعاقدية مع البنك.

وقد تعاضمت أهمية الخصوصية في القطاع المصرفي مع صدور تشريعات حماية البيانات على المستوى الدولي مثل اللائحة العامة لحماية البيانات الأوروبية (GDPR) ، وعلى المستوى المحلي مثل نظام حماية البيانات الشخصية في المملكة العربية السعودية الذي أرسى إطاراً قانونياً واضحاً يلزم المؤسسات بالوصول على موافقة صريحة من الأفراد قبل جمع بياناتهم ومعالجتها، ويمنحهم حق الوصول إليها وتصحيحها وحذفها. وتتحقق الخصوصية من خلال تبني مبادئ الخصوصية بالتصميم (Privacy by Design) التي تدمج متطلبات الخصوصية في بنية الأنظمة منذ مرحلة التصميم، فضلاً عن تقنيات إخفاء البيانات (Data Masking) والترميز (Tokenization) والتشفير المتجانس (Homomorphic Encryption) الذي يسمح بمعالجة البيانات وهي مشفرة.

وقد أكدت دراسة (Sebihi et al. (2024 أن الخصوصية تُعد من أقوى المحددات المؤثرة في ثقة العملاء بالخدمات المالية الرقمية، لا سيما في ظل تنامي وعي المستهلكين بحقوقهم المتعلقة ببياناتهم الشخصية. كما بيّنت دراسة عبد الفاتح (2022) أن إدراك العملاء لإجراءات حماية خصوصيتهم يرتبط بمستوى ثقتهم في التعاملات المصرفية الإلكترونية. وأوضحت دراسة الغامدي والمصطفي (2021) أن

الخصوصية تتفاعل مع بقية أبعاد الأمن السيبراني لتشكيل تصور متكامل لدى المستخدمين حول مستوى الحماية المقدمة، مما يؤكد ضرورة التعامل معها كُبعد مستقل وليس كجزء من السرية.

6.1.2 استراتيجيات الأمن السيبراني في القطاع المصرفي

تتبنى المؤسسات المصرفية مجموعة من الاستراتيجيات لتحقيق أهداف الأمن السيبراني وحماية بنيتها التحتية الرقمية وبيانات عملائها. وتتنوع هذه الاستراتيجيات بين ما هو وقائي واستباقي وما هو تفاعلي وعلاجي، وتعمل في مجملها ضمن إطار متكامل يُشكّل منظومة الدفاع السيبراني للبنك.

تُعد استراتيجية الدفاع في العمق (Defense in Depth) من أبرز الاستراتيجيات المتبعة في القطاع المصرفي، وهي تقوم على مبدأ إنشاء طبقات أمنية متعددة ومتتالية بحيث لا يعتمد أمن المؤسسة على خط دفاع واحد. وقد أشار زريقات والحوامده (2022) إلى أن هذه الاستراتيجية تشمل في البيئة المصرفية طبقة أمن الشبكات التي تتضمن جدران الحماية وأنظمة منع التسلل، وطبقة أمن التطبيقات التي تشمل اختبار الاختراق ومراجعة الشفرة البرمجية، وطبقة أمن البيانات التي تتضمن التشفير وإدارة المفاتيح، وطبقة أمن المستخدم النهائي التي تشمل المصادقة القوية والتوعية الأمنية. ويكمن جوهر هذه الاستراتيجية في أنه حتى لو تم اختراق إحدى الطبقات، فإن الطبقات الأخرى تظل قادرة على احتواء التهديد ومنع وصوله إلى الأصول الحرجة.

وتبرز استراتيجية إدارة المخاطر السيبرانية (Cyber Risk Management) كإطار منهجي يتبناه البنك لتحديد التهديدات المحتملة وتقييم احتمالية وقوعها وأثرها، ثم وضع الضوابط المناسبة للحد من هذه المخاطر أو نقلها أو قبولها. وقد أكد الهلسه والشيخ (2021) أن إدارة المخاطر السيبرانية في البنوك يجب أن تتكامل مع إطار إدارة المخاطر المؤسسية الشامل، بحيث تُعالج المخاطر السيبرانية بنفس المنهجية والجدية التي تُعالج بها المخاطر الائتمانية والتشغيلية والسوقية. كما أشارت دراسة البوانه وصالح (2023) إلى أن تقييم مخاطر الأمن السيبراني في المؤسسات المالية يتطلب منهجية تأخذ بعين الاعتبار خصوصية القطاع المصرفي وتعقيد بنيته التقنية.

كما تتبنى البنوك السعودية استراتيجية الامتثال التنظيمي (Regulatory Compliance) التي تستند إلى الأطر والمعايير التي وضعتها الجهات الرقابية. وفي هذا الصدد، أصدر البنك المركزي السعودي إطار الأمن السيبراني (SAMA Cybersecurity Framework) الذي يلزم جميع المؤسسات المالية الخاضعة لإشرافه بتطبيق مجموعة شاملة من الضوابط الأمنية. كما تؤدي الهيئة الوطنية للأمن السيبراني دورًا محوريًا من خلال الضوابط الأساسية للأمن السيبراني التي تُطبّق على جميع الجهات الحكومية والقطاع الخاص. وقد أكدت دراسة الغامدي والمصطفي (2021) أن الامتثال لهذه المعايير لا يُعد مجرد التزام تنظيمي، بل يُشكّل ميزة تنافسية تُعزز ثقة العملاء والشركاء في المؤسسة.

وتحتل استراتيجية الاستجابة للحوادث (Incident Response) مكانة مهمة في منظومة الأمن السيبراني المصرفي، إذ تنطلق من مبدأ أنه مهما بلغت قوة الدفاعات الأمنية، فإن احتمال وقوع حادثة أمنية يظل قائمًا. ولذلك تُعد البنوك خططًا تفصيلية للاستجابة تتضمن مراحل الكشف والاحتواء والاستئصال والتعافي والدروس المستفادة. وقد أوضحت حسين وأبو الغنم (2022) أن سرعة وفعالية الاستجابة للحوادث الأمنية تؤثر بشكل مباشر في مدى تأثير سمعة البنك، إذ يمكن لاستجابة سريعة وشفافة أن تحدّ من الأضرار وتحافظ على ثقة العملاء حتى في حالة وقوع الاختراق.

فضلاً عن ذلك، تتنامى أهمية استراتيجية التوعية والتدريب الأمني التي تستهدف بناء الوعي السيبراني لدى الموظفين والعملاء على حد سواء. وقد أكد عبد الفاتح (2022) أن العنصر البشري يُمثّل الحلقة الأضعف في سلسلة الأمن السيبراني، وأن رفع مستوى الوعي لدى العملاء بأساليب الاحتيال الإلكتروني والتصيد يُسهم بشكل فعال في تقليل المخاطر وتعزيز الحماية الشاملة للمنظومة المصرفية.

7.1.2 التحديات المعاصرة للأمن السيبراني المصرفي

تواجه المؤسسات المصرفية جملة من التحديات التي تُعقّد مهمة تأمين بيئتها الرقمية وتفرض عليها تطويرًا مستمرًا لقدراتها الأمنية. ومن أبرز هذه التحديات تطور أساليب الهجوم السيبراني وتزايد تعقيدها، حيث لم تعد التهديدات تقتصر على الفيروسات التقليدية أو محاولات الاختراق البسيطة، بل باتت تشمل

هجمات التهديد المتقدم والمستمر (APT) التي تستهدف مؤسسات بعينها وتستخدم تقنيات معقدة للتخفي داخل الشبكات لفترات طويلة.

كما يُمثل التوفيق بين متطلبات الأمن وسهولة الاستخدام تحديًا دائمًا، إذ قد تؤدي الإجراءات الأمنية المشددة إلى تعقيد تجربة المستخدم ودفعه نحو البحث عن بدائل أقل أمنًا لكنها أسهل استخدامًا. ويُضاف إلى ذلك تحدي النقص في الكوادر المتخصصة في الأمن السيبراني، وهو تحدٍ عالمي تتفاقم حدته في المنطقة العربية. وقد أشار العبد اللات والشورة (2023) إلى أن اندماج التقنيات المالية الحديثة (FinTech) مع الأنظمة المصرفية التقليدية يخلق سطح هجوم أوسع ويتطلب مقاربات أمنية جديدة. كما أوضحت دراسة (Amer and Al-Omar (2023 أن تبني تقنيات البلوك تشين وإن كان يوفر مزايا أمنية، إلا أنه يطرح تحديات تتعلق بحوكمة البيانات والامتثال التنظيمي تستوجب معالجة مدروسة.

المبحث الثاني: ثقة العملاء في المعاملات البنكية الإلكترونية

1.2.2 تمهيد

تُعد الثقة من أكثر المفاهيم محورية في العلاقات الإنسانية والتجارية، وقد ازدادت أهميتها في البيئة الرقمية التي تتسم بغياب التفاعل الشخصي المباشر وتعاضل حالة عدم اليقين لدى المتعاملين. وفي السياق المصرفي الإلكتروني، تكتسب الثقة بُعدًا خاصًا، إذ يُطلب من العميل أن يُفوض البنك — عبر منصة رقمية — بإدارة أمواله وبياناته الشخصية دون أن يكون هناك تواصل بشري مباشر يُطمئنه ويُبدد مخاوفه. ويتناول هذا المبحث مفهوم ثقة العملاء وتعريفاته في الأدبيات الأكاديمية، ثم ينتقل إلى أهميتها في بيئة الخدمات المصرفية الإلكترونية وأهدافها ومحدداتها واستراتيجيات بنائها وتعزيزها، مع الربط بمتغير الأمن السيبراني باعتباره أحد العوامل المؤثرة فيها.

2.2.2 مفهوم ثقة العملاء

حظي مفهوم الثقة باهتمام واسع من الباحثين في تخصصات متعددة تشمل علم النفس والاجتماع والتسويق وإدارة الأعمال ونظم المعلومات، مما أفرز تعددًا في تعريفاته يعكس ثراء المفهوم وتشعب أبعاده. فمن المنظور النفسي، تُعرّف الثقة بأنها حالة نفسية تتضمن استعداد الفرد لقبول الضعف بناءً على توقعات إيجابية حول نوايا وسلوكيات الطرف الآخر. وقد انتقل هذا المفهوم إلى ميدان إدارة الأعمال ليُوظّف في فهم العلاقة بين المؤسسة وعملائها.

وفي السياق التسويقي، عرّفت دراسة حسين وأبو الغنم (2022) ثقة العملاء بأنها اعتقاد العميل بأن المؤسسة ستتصرف بما يخدم مصلحته وتفي بالتزاماتها تجاهه بصورة متسقة ومستمرة، وأن هذا الاعتقاد ينشأ نتيجة تراكم الخبرات الإيجابية والتفاعلات الناجحة مع المؤسسة عبر الزمن. ويُبرز هذا التعريف البُعد التراكمي للثقة وارتباطها بالتجربة الفعلية وليس بالوعود المجردة.

أما في مجال الخدمات المصرفية الإلكترونية تحديداً، فقد عرّفها العبد اللات والشورة (2023) بأنها درجة اطمئنان العميل واستعداده للاعتماد على القنوات الرقمية للبنك في إجراء معاملاته المالية، وهذا الاطمئنان ينبثق من إدراكه لمستوى الأمان والكفاءة والموثوقية الذي توفره هذه القنوات. ويتميز هذا التعريف بربطه المباشر بين الثقة وأبعاد الأمن السيبراني، مما يجعله أقرب إلى التأطير النظري للدراسة الحالية.

وقد تناول عبد الفاتح (2022) المفهوم من زاوية وعي العميل، حيث عرّف الثقة المصرفية الإلكترونية بأنها المحصلة الإدراكية لتقييم العميل لقدرة البنك على حماية بياناته وأمواله في البيئة الرقمية، وأن هذه المحصلة تتشكل من خلال معارف العميل ومهاراته وخبراته في التعامل مع التقنية. ويُضيف هذا التعريف بُعداً معرفياً مهماً، إذ يجعل مستوى الثقة مرتبطاً بمستوى الوعي الرقمي للعميل.

كما عرّفها Sebihi et al. (2024) بأنها التقييم الشامل الذي يُجرّيه العميل لدى جدارة مقدم الخدمة المالية الرقمية بالاعتماد عليه، وأن هذا التقييم يتأسس على ثلاثة أركان: الكفاءة المدركة في تقديم الخدمة، والنزاهة المدركة في التعامل مع بيانات العميل، والإحسان المدرك في مراعاة مصلحة العميل. أما Krishna et al. (2025) فقد عرّفها بأنها الاستعداد السلوكي للعميل للاعتماد على الخدمة الرقمية في المعاملات المالية الحساسة، وأن هذا الاستعداد يتأثر بشكل مباشر بتجربة الاستخدام ومستوى الموثوقية التقنية المدركة.

وعرّفت دراسة البوانه وصالح (2023) ثقة العميل المصرفي بأنها قناعته بأن البنك يمتلك الإمكانيات التقنية والتنظيمية الكافية لحمايته من المخاطر السيبرانية التي قد تنجم عن استخدامه للخدمات المصرفية الإلكترونية. ويتميز هذا التعريف بتركيزه على البُعد الأمني للثقة وارتباطها بإدراك العميل لمخاطر التعامل الإلكتروني.

وفي ضوء هذه التعريفات المتنوعة، يرى الباحث أن ثقة العملاء في المعاملات البنكية الإلكترونية يمكن تعريفها بأنها حالة إدراكية ووجدانية وسلوكية تعكس اطمئنان العميل واستعداده للاعتماد على القنوات الرقمية للبنك في إجراء معاملاته المالية، بناءً على تقييمه الشامل لمستوى الأمن السيبراني المتحقق

في هذه القنوات من حيث السرية والسلامة والموثوقية والخصوصية. ويجمع هذا التعريف بين الأبعاد المعرفية والعاطفية والسلوكية للثقة، ويربطها بأبعاد المتغير المستقل في الدراسة الحالية.

3.2.2 أهمية ثقة العملاء في الخدمات المصرفية الإلكترونية

تحتل الثقة مكانة محورية في نجاح الخدمات المصرفية الإلكترونية واستدامتها، إذ تُعد المحرك الأساسي لتبني العملاء لهذه الخدمات واستمرارهم في استخدامها. وفي غياب التفاعل البشري المباشر الذي يُميز العلاقة المصرفية التقليدية، تصبح الثقة البديل الوحيد الذي يُبذل مخاوف العميل ويُشجعه على تفويض البنك بإدارة شؤونه المالية عبر الفضاء الرقمي.

وتشير دراسة حسين وأبو الغنم (2022) إلى أن أهمية الثقة في البيئة المصرفية تتجلى في عدة أبعاد:

- تُعد الثقة شرطاً مسبقاً لتبني العميل للخدمات المصرفية الإلكترونية، فالعمليل الذي لا يثق في أمان المنصة الرقمية لن يُقدم على استخدامها مهما بلغت سهولتها أو فوائدها.
- تُسهم الثقة في تقليل المخاطر المدركة لدى العميل، حيث تعمل كآلية تعويضية تُوازن الشعور بعدم اليقين المصاحب للمعاملات الإلكترونية.
- تؤثر الثقة في نوايا العميل السلوكية من حيث الاستمرار في استخدام الخدمة والتوصية بها للآخرين وزيادة حجم التعاملات.

ويرى زريقات والحوامده (2022) أن أهمية الثقة تتعاظم في سياق التجارة الإلكترونية المصرفية الدولية، حيث:

- تُشكّل الثقة العامل الحاسم في قبول العملاء للتعامل مع مؤسسات مالية عبر الحدود، في ظل اختلاف الأنظمة القانونية وتعدد المخاطر.
- تُعد الثقة عنصراً أساسياً في تقليل تكاليف المعاملات، إذ يُقلل العميل الواثق من إجراءات التحقق والمراجعة التي يقوم بها قبل كل عملية.

- تُسهم الثقة في بناء علاقات طويلة الأمد بين البنك وعملائه، مما يُقلل معدل انتقال العملاء إلى بنوك منافسة.

كما يؤكد العبداللات والشورة (2023) أن أهمية الثقة تبرز بقوة في المنظور التسويقي:

- تُعد الثقة أحد أقوى محددات ولاء العملاء في البيئة الرقمية، وهي تتفوق على عوامل أخرى كالسعر وتنوع الخدمات في التأثير على قرار الاستمرار.
- تُشكّل الثقة ميزة تنافسية يصعب على المنافسين تقليدها، لكونها نتاج تراكم خبرات وتفاعلات إيجابية لا يمكن بناؤها في وقت قصير.
- تؤثر الثقة في استعداد العميل لمشاركة بياناته مع البنك، وهي بيانات ضرورية لتخصيص الخدمات وتحسين تجربة المستخدم.

4.2.2 أهداف بناء ثقة العملاء في البيئة المصرفية الرقمية

تسعى المؤسسات المصرفية من خلال بناء ثقة عملائها إلى تحقيق جملة من الأهداف الاستراتيجية والتشغيلية التي تناولها الباحثون من زوايا متعددة.

فقد حددت دراسة حسين وأبو الغنم (2022) أهدافاً تتمحور حول العلاقة بين البنك والعميل :

- تحويل العملاء من القنوات التقليدية إلى القنوات الرقمية بما يُقلل تكلفة الخدمة ويزيد كفاءتها
 - تعزيز ولاء العملاء وتقليل معدل الانتقال إلى المنافسين .
 - زيادة حجم التعاملات الإلكترونية وتنويعها بما يشمل العمليات عالية القيمة.
- أما دراسة العبداللات والشورة (2023) فقد ركزت على الأهداف التسويقية
- بناء سمعة رقمية قوية للبنك تُسهم في استقطاب عملاء جدد عبر التوصية الشفهية الإلكترونية .
 - تمكين البنك من تقديم خدمات مبتكرة تتطلب مستوى عالٍ من ثقة العملاء، كالمحافظ الرقمية والاستثمار الإلكتروني .

- تحسين صورة البنك الذهنية لدى العملاء المحتملين بما يُقلل تكلفة الاستحواذ.

وأضافت دراسة عبد الفاتح (2022) أهدافاً مرتبطة بالوعي والتمكين :

- تمكين العملاء من المشاركة الفعالة في حماية حساباتهم من خلال رفع وعيهم الأمني .
- تقليل حالات الاحتيال والتصيد الإلكتروني الناتجة عن ضعف ثقة العملاء وجهلهم بالإجراءات الأمنية .
- بناء علاقة شراكة بين البنك والعميل قائمة على الشفافية والمسؤولية المشتركة.

5.2.2 محددات ثقة العملاء في المعاملات البنكية الإلكترونية

تتشكل ثقة العملاء في المعاملات البنكية الإلكترونية من خلال تفاعل مجموعة من المحددات التي يمكن تصنيفها في أربع فئات رئيسية تُشكّل في مجملها الإطار الذي يُقيّم العميل من خلاله مدى جدارة البنك بالثقة.

تتمثل الفئة الأولى في المحددات المتعلقة بسمعة البنك وتاريخه، حيث يميل العملاء إلى الثقة في البنوك ذات السمعة الراسخة والتاريخ الطويل في السوق. وقد أوضحت دراسة حسين وأبو الغنم (2022) أن سمعة البنك تُعد من أقوى المؤشرات التي يعتمد عليها العملاء في تكوين انطباعاتهم الأولية، لا سيما العملاء الجدد الذين لا تتوفر لديهم خبرة سابقة مع المؤسسة. وتشكل السمعة من عدة عناصر تشمل الأداء المالي والالتزام الأخلاقي وتاريخ التعامل مع الأزمات والحضور الإعلامي والمسؤولية الاجتماعية.

وتتمثل الفئة الثانية في المحددات التقنية والأمنية، وهي المحددات الأكثر ارتباطاً بموضوع الدراسة الحالية. وتشمل هذه المحددات مستوى الأمن السيبراني المُدرك بأبعاده الأربعة — السرية والسلامة والموثوقية والخصوصية — فضلاً عن جودة تصميم المنصة الرقمية وسهولة استخدامها وسرعة أداؤها. وقد أكد كل من الغامدي والمصطفي (2021) و Sebihi et al. (2024) أن العوامل التقنية والأمنية تُشكّل المحدد الأكثر تأثيراً في ثقة العملاء بالخدمات الرقمية، خاصة في المعاملات المالية التي تنطوي على مخاطر عالية.

أما الفئة الثالثة فتتعلق بالمحددات المرتبطة بالعمل ذاته، وتشمل مستوى ثقافته الرقمية وخبرته السابقة في التعامل مع التقنية واتجاهاته العامة نحو الابتكار التكنولوجي. وقد بينت دراسة عبد الفاتح (2022) أن العملاء الأكثر وعيًا بالتقنية وأساليب الحماية يميلون إلى مستويات أعلى من الثقة في التعاملات الإلكترونية، مما يعني أن التوعية الأمنية للعملاء تُعد استثمارًا مباشرًا في بناء الثقة.

وتتمثل الفئة الرابعة في المحددات البيئية والتنظيمية، وتشمل وجود إطار تشريعي وتنظيمي فعال يحمي حقوق المتعاملين ويُلزم المؤسسات المالية بمعايير أمنية محددة. وفي هذا السياق، تتميز البيئة السعودية بوجود منظومة تنظيمية متقدمة يُشرف عليها البنك المركزي السعودي والهيئة الوطنية للأمن السيبراني، مما يُشكّل بيئة مؤسسية داعمة لبناء ثقة العملاء. وقد أشار زريقات والحوامده (2022) إلى أن وجود إطار حوكمي واضح للأمن السيبراني يُعزز ثقة العملاء ليس فقط في البنك الذي يتعاملون معه، بل في المنظومة المصرفية ككل.

6.2.2 استراتيجيات بناء وتعزيز ثقة العملاء

تتبنى المؤسسات المصرفية استراتيجيات متنوعة لبناء ثقة عملائها في القنوات الرقمية وتعزيزها، وتتكامل هذه الاستراتيجيات فيما بينها لتُشكّل مقاربة شمولية تأخذ بعين الاعتبار تنوع محددات الثقة وتعدد أبعادها.

تبرز في المقام الأول استراتيجية تعزيز الأمن السيبراني المُدرك، والتي لا تقتصر على تطبيق إجراءات أمنية فعلية، بل تمتد لتشمل إيصال هذه الإجراءات للعملاء بشكل واضح ومفهوم. فقد أشارت دراسة Sebihi et al. (2024) إلى أن الفجوة بين مستوى الأمان الفعلي ومستوى الأمان المُدرك لدى العميل يمكن أن تُقوّض الثقة حتى لو كانت البنية الأمنية متقدمة. ولذلك تسعى البنوك إلى عرض شهادات الأمان والتصنيفات المعتمدة على منصات الرقمية، وتوضيح إجراءات الحماية المتبعة بلغة بسيطة يفهمها العميل العادي.

وتحتل استراتيجية الشفافية والتواصل مكانة بارزة في بناء الثقة، حيث تعتمد على إطلاع العملاء بشكل استباقي على أي تطورات تتعلق بأمن حساباتهم وبياناتهم. وقد أكدت حسين وأبو الغنم (2022) أن الشفافية في التعامل مع الحوادث الأمنية — عند وقوعها — تُسهم في الحفاظ على ثقة العملاء بدلاً من محاولة التستر التي قد تُحدث ضرراً أكبر عند انكشاف الحقيقة. كما تشمل هذه الاستراتيجية وضوح سياسات الخصوصية وشروط الاستخدام وآليات معالجة الشكاوى.

كما تتبنى البنوك استراتيجية بناء تجربة استخدام متسقة وموثوقة، تقوم على ضمان أداء مستقر وخالٍ من الأعطال للمنصات الرقمية، وتوفير واجهة استخدام بديهية ومريحة، وتقديم دعم فني فوري عند الحاجة. وقد أوضح (Krishna et al. (2025 أن اتساق تجربة الاستخدام عبر الزمن يُرسّخ الثقة بشكل تراكمي، في حين أن تجربة سلبية واحدة قد تُقوّض ثقة بُنيت على مدى فترة طويلة.

فضلاً عن ذلك، تتنامى أهمية استراتيجية الامتثال التنظيمي والاعتماد كأداة لبناء الثقة، حيث تسعى البنوك إلى الحصول على شهادات واعتمادات أمنية معترف بها دولياً مثل ISO 27001 والتوافق مع إطار الأمن السيبراني للبنك المركزي السعودي، وعرض هذه الاعتمادات على عملائها كدليل موثوق على التزامها بأعلى المعايير الأمنية. وقد أشار الهلسه والشيخ (2021) إلى أن التوافق مع الأطر المعيارية الدولية يُعزز مصداقية المؤسسة المالية ويُرسّخ ثقة أصحاب المصلحة في مخرجاتها.

7.2.2 العلاقة النظرية بين الأمن السيبراني وثقة العملاء

يمكن تأطير العلاقة بين الأمن السيبراني وثقة العملاء من خلال عدة مداخل نظرية تُعزز الأساس الأكاديمي لهذه الدراسة. فمن منظور نظرية المخاطر المدركة، يُقلل كل بُعد من أبعاد الأمن السيبراني من نوع محدد من المخاطر التي يدركها العميل: فالسرية تُقلل مخاطر كشف البيانات، والسلامة تُقلل مخاطر التلاعب بالمعاملات، والموثوقية تُقلل مخاطر انقطاع الخدمة، والخصوصية تُقلل مخاطر إساءة استخدام البيانات الشخصية. وكلما انخفضت المخاطر المدركة ارتفع مستوى الثقة.

ومن منظور نظرية الإشارات (Signaling Theory) ، تعمل إجراءات الأمن السيبراني المدركة كإشارات يُرسلها البنك للعملاء تدل على كفاءته والتزامه وجدارته بالثقة. وقد أشارت دراسة الغامدي والمصطدي (2021) إلى أن المؤسسات التي تستثمر في بنيتها الأمنية ترسل إشارة قوية لأصحاب المصلحة بأنها تُولي أولوية لحماية مصالحهم. أما من منظور نموذج قبول التقنية (TAM) ، فإن الأمن السيبراني يُعزز الفائدة المدركة وسهولة الاستخدام المدركة للخدمة المصرفية الإلكترونية، مما ينعكس إيجابًا على نية الاستخدام التي تتوسط فيها الثقة كعامل حاسم.

وقد أكدت دراسة عبد الفاتح (2022) أن وعي العملاء بإجراءات الأمن السيبراني المتبعة في البنوك يُعزز ثقتهم بشكل مباشر ويُقلل من مخاوفهم الأمنية. كما أوضحت دراسة (Sebihi et al. 2024) أن الأبعاد الأمنية تعمل بشكل تكاملي وليس تنافسيًا في بناء الثقة، بمعنى أن ضعف أي بُعد من الأبعاد قد يُقوّض الأثر الإيجابي للأبعاد الأخرى.

الفصل الثالث: منهجية الدراسة

1.3 تمهيد

يتناول هذا الفصل الإجراءات المنهجية التي اتبعتها الدراسة لتحقيق أهدافها واختبار فرضياتها، وذلك من خلال تحديد المنهج العلمي المستخدم، ووصف مجتمع الدراسة وعينتها وأسلوب اختيارها، وبناء أداة الدراسة (الاستبانة) وتوضيح مكوناتها ومحاورها، ثم التحقق من صدق الأداة وثباتها باستخدام الأساليب الإحصائية المناسبة، وأخيراً عرض الأساليب الإحصائية المعتمدة في تحليل البيانات واختبار الفرضيات.

2.3 منهج الدراسة

اعتمدت الدراسة الحالية على المنهج الوصفي التحليلي بوصفه المنهج الأكثر ملاءمة لطبيعة الدراسة وأهدافها، حيث يسعى هذا المنهج إلى وصف الظاهرة محل الدراسة كما هي في الواقع وتحليلها وتفسيرها والكشف عن العلاقات بين متغيراتها. وقد استُخدم هذا المنهج في شقّه الوصفي لوصف واقع الأمن السيبراني وأبعاده في المصارف السعودية ومستوى ثقة العملاء في المعاملات البنكية الإلكترونية، وفي شقّه التحليلي لاختبار أثر أبعاد الأمن السيبراني (سرية المعلومات، سلامة النظام، الموثوقية، الخصوصية) على ثقة العملاء، وذلك من خلال جمع البيانات الأولية باستخدام الاستبانة كأداة رئيسة.

3.3 مجتمع الدراسة وعينتها

مجتمع الدراسة

يتكون مجتمع الدراسة من عملاء المصارف السعودية الذين يستخدمون الخدمات المصرفية الإلكترونية (الخدمات المصرفية عبر الإنترنت، تطبيقات الهاتف المحمول، أجهزة الصراف الآلي، نقاط البيع

الإلكترونية) في المملكة العربية السعودية. ونظراً لكبر حجم المجتمع وصعوبة حصره بشكل دقيق، فقد تم اعتباره مجتمعاً غير محدود.

عينة الدراسة

اعتمدت الدراسة على أسلوب العينة العشوائية الميسرة (Convenience Random Sampling) في اختيار عينة الدراسة من عملاء المصارف السعودية الذين يستخدمون الخدمات المصرفية الإلكترونية. وبناءً على معادلة تحديد حجم العينة للمجتمعات غير المحدودة، وباستخدام مستوى ثقة 95% وهامش خطأ 5%، فإن الحد الأدنى المطلوب لحجم العينة يبلغ (384) مفردة. وقد تم توزيع (450) استبانة لضمان الحصول على عدد كافٍ من الاستجابات الصالحة للتحليل الإحصائي، وبعد الفرز والمراجعة تم استبعاد (26) استبانة لعدم اكتمال البيانات أو وجود أنماط إجابة غير منطقية، ليصبح عدد الاستبانات الصالحة للتحليل (424) استبانة بمعدل استجابة بلغ (94.2%).

جدول (1) توزيع الاستبانات ومعدل الاستجابة

البيان	العدد	النسبة
الاستبانات الموزعة	450	100%
الاستبانات المستردة	436	96.9%
الاستبانات المستبعدة (غير صالحة)	12	2.7%
الاستبانات غير المستردة	14	3.1%
الاستبانات الصالحة للتحليل	424	94.2%

4.3 أداة الدراسة (الاستبانة)

اعتمدت الدراسة على الاستبانة كأداة رئيسة لجمع البيانات الأولية، وقد تمّ تصميمها بناءً على مراجعة الأدبيات والدراسات السابقة ذات الصلة بمتغيرات الدراسة. وتكونت الاستبانة من ثلاثة أقسام رئيسة:

- ❖ القسم الأول: البيانات الديموغرافية، ويتضمن (5) فقرات تتعلق بالنوع والفئة العمرية والمؤهل العلمي ومدة الاستخدام ومعدل تكرار الاستخدام.
- ❖ القسم الثاني: المتغير المستقل (الأمن السيبراني)، ويتكون من (16) فقرة موزعة على أربعة أبعاد بواقع (4) فقرات لكل بُعد.
- ❖ القسم الثالث: المتغير التابع (ثقة العملاء في المعاملات البنكية الإلكترونية)، ويتكون من (12) فقرة في محور واحد.

وقد تمّ قياس جميع فقرات القسمين الثاني والثالث باستخدام مقياس ليكرت الخماسي المتدرج من (1) إلى (5) حيث: (1) غير موافق بشدة، (2) غير موافق، (3) محايد، (4) موافق، (5) موافق بشدة.

هيكل أداة الدراسة

جدول (2): توزيع فقرات الاستبانة على محاور الدراسة

المحور	البُعد / المتغير	أرقام الفقرات	عدد الفقرات
القسم الأول	البيانات الديموغرافية	—	5
القسم الثاني	المتغير المستقل: الأمن السيبراني		16
	البُعد الأول: سرية المعلومات	1 – 4	4
	البُعد الثاني: سلامة النظام	5 – 8	4
	البُعد الثالث: الموثوقية	9 – 12	4

4	13 – 16	البُعد الرابع: الخصوصية	
12	17 – 28	المتغير التابع: ثقة العملاء	القسم الثالث
33فقرة		الإجمالي	

5.3 صدق أداة الدراسة

تمّ التحقق من صدق أداة الدراسة من خلال نوعين من الصدق: الصدق الظاهري (صدق المحكمين)، وصدق الاتساق الداخلي (صدق البناء).

أ. الصدق الظاهري (صدق المحكمين)

تمّ عرض الاستبانة في صورتها الأولية على مجموعة من المحكمين المتخصصين من أعضاء هيئة التدريس في تخصصات إدارة الأعمال ونظم المعلومات الإدارية والتسويق، وقد بلغ عددهم (7) محكمين. وقد طُلب منهم إبداء آرائهم حول مدى ملاءمة الفقرات لقياس ما وُضعت لقياسه، ووضوح الصياغة اللغوية، وانتماء كل فقرة لبُعدها، وكفاية عدد الفقرات. وفي ضوء ملاحظات المحكمين، تمّ إعادة صياغة بعض الفقرات لتحسين وضوحها، وتعديل ترتيب بعض الفقرات لتحقيق تسلسل منطقي أفضل، مع الإبقاء على العدد الكلي للفقرات كما هو.

ب. مصفوفة الارتباط بين أبعاد الدراسة

تمّ حساب مصفوفة معاملات ارتباط بيرسون بين أبعاد المتغير المستقل والمتغير التابع للتحقق من وجود علاقات ارتباطية بين متغيرات الدراسة ومن عدم وجود ازدواج خطي (Multicollinearity) بين المتغيرات المستقلة.

جدول (3): مصفوفة معاملات الارتباط بين متغيرات الدراسة

المتغير	سرية المعلومات	سلامة النظام	الموثوقية	الخصوصية	ثقة العملاء
سرية المعلومات	1.000				
سلامة النظام	0.614**	1.000			
الموثوقية	0.583**	0.647**	1.000		
الخصوصية	0.691**	0.572**	0.608**	1.000	
ثقة العملاء	0.713**	0.682**	0.729**	0.697**	1.000

**دالة إحصائية عند مستوى (0.01)

يتبين من مصفوفة الارتباط أن جميع معاملات الارتباط بين أبعاد المتغير المستقل والمتغير التابع دالة إحصائية عند مستوى (0.01)، وأن قيمها تراوحت بين (0.682) و(0.729) مما يُشير إلى وجود علاقات ارتباطية موجبة وقوية بين أبعاد الأمن السيبراني وثقة العملاء. كما يتبين أن معاملات الارتباط بين الأبعاد المستقلة فيما بينها تراوحت بين (0.572) و(0.691) وهي أقل من (0.80)، مما يُشير إلى عدم وجود مشكلة ازدواج خطي بين المتغيرات المستقلة ويُجيز استخدامها معاً في نماذج الانحدار المتعدد.

6.3 ثبات أداة الدراسة

تمّ التحقق من ثبات أداة الدراسة باستخدام معامل ألفا كرونباخ (Cronbach's Alpha) الذي يقيس مدى الاتساق الداخلي لفقرات كل بُعد وفقرات الأداة ككل، وذلك باستخدام بيانات العينة الاستطلاعية (ن = 40).

جدول (4): معاملات ثبات ألفا كرونباخ لأبعاد الدراسة

المحور / البُعد	عدد الفقرات	معامل ألفا كرونباخ
سرية المعلومات	4	0.863

المحور / البُعد	عدد الفقرات	معامل ألفا كرونباخ
سلامة النظام	4	0.879
الموثوقية	4	0.854
الخصوصية	4	0.871
إجمالي المتغير المستقل (الأمن السيبراني)	16	0.924
ثقة العملاء في المعاملات البنكية الإلكترونية	12	0.937
الأداة ككل	28	0.951

يتضح من الجدول أن قيم معامل ألفا كرونباخ لجميع أبعاد الدراسة تراوحت بين (0.854) و(0.879) وهي قيم مرتفعة تتجاوز الحد المقبول (0.70)، كما بلغ معامل الثبات الكلي للأداة (0.951) وهو معامل مرتفع جداً يُشير إلى درجة عالية من الاتساق الداخلي والثبات، مما يُعزز الثقة في قدرة الأداة على إعطاء نتائج مستقرة ومتسقة عند إعادة تطبيقها في ظروف مماثلة.

7.3 الأساليب الإحصائية المستخدمة

استُخدمت مجموعة من الأساليب الإحصائية لتحليل بيانات الدراسة واختبار فرضياتها، وذلك من خلال برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS)، وتشمل هذه الأساليب ما يلي:

- التكرارات والنسب المئوية: لوصف خصائص عينة الدراسة الديموغرافية.
- المتوسطات الحسابية والانحرافات المعيارية: لتحديد مستوى استجابات أفراد العينة على فقرات الاستبانة وأبعادها وترتيب الأبعاد وفقاً لأهميتها النسبية.
- معامل ارتباط بيرسون (Pearson Correlation): للتحقق من صدق الاتساق الداخلي لأداة الدراسة وقياس العلاقات الارتباطية بين متغيرات الدراسة.
- معامل ألفا كرونباخ (Cronbach's Alpha): للتحقق من ثبات أداة الدراسة ومستوى اتساقها الداخلي.

- معامل تضخم التباين (VIF) واختبار التباين المسموح (Tolerance) للتحقق من عدم وجود مشكلة ازدواج خطي بين المتغيرات المستقلة قبل إجراء تحليل الانحدار.
- تحليل الانحدار الخطي البسيط (Simple Linear Regression): لاختبار أثر كل بُعد من أبعاد الأمن السيبراني على ثقة العملاء بشكل منفرد، وذلك لاختبار الفرضيات الفرعية الأربع.
- تحليل الانحدار الخطي المتعدد (Multiple Linear Regression): لاختبار الأثر المشترك لأبعاد الأمن السيبراني مجتمعة على ثقة العملاء، وذلك لاختبار الفرض الرئيس وتحديد الأهمية النسبية لكل بُعد في تفسير التباين في ثقة العملاء.

الفصل الرابع: تحليل البيانات واختبار الفرضيات

1.4 تحليل البيانات الديموغرافية لأفراد العينة

جدول (5): توزيع أفراد العينة وفقاً للنوع

النوع	التكرار	النسبة المئوية
ذكر	247	58.3%
أنثى	177	41.7%
الإجمالي	424	100%

يتضح من الجدول أن غالبية أفراد العينة من الذكور بنسبة (58.3%)، بينما بلغت نسبة الإناث (41.7%). ويُشير هذا التوزيع إلى تمثيل مقبول لكلا الجنسين في العينة مع تفوق نسبي للذكور، وهو ما يتسق مع الواقع الديموغرافي لمستخدمي الخدمات المصرفية الإلكترونية في المملكة العربية السعودية.

جدول (6): توزيع أفراد العينة وفقاً للفئة العمرية

الفئة العمرية	التكرار	النسبة المئوية
أقل من 25 سنة	68	16.0%
من 25 إلى أقل من 35 سنة	139	32.8%
من 35 إلى أقل من 45 سنة	118	27.8%
من 45 إلى أقل من 55 سنة	64	15.1%
55 سنة فأكثر	35	8.3%
الإجمالي	424	100%

يُظهر الجدول أن الفئة العمرية الأكثر تمثيلاً هي فئة (25 إلى أقل من 35 سنة) بنسبة (32.8%)، تليها فئة (35 إلى أقل من 45 سنة) بنسبة (27.8%)، ثم فئة (أقل من 25 سنة) بنسبة (16.0%). ويدل ذلك على أن ما يزيد عن ثلاثة أرباع العينة (76.6%) تقع أعمارهم دون (45) سنة، مما يعكس أن الشرائح العمرية الشابة والمتوسطة هي الأكثر استخداماً للخدمات المصرفية الإلكترونية.

جدول (7): توزيع أفراد العينة وفقاً للمؤهل العلمي

المؤهل العلمي	التكرار	النسبة المئوية
ثانوية عامة أو أقل	52	12.3%
دبلوم	71	16.7%
بكالوريوس	213	50.2%
دراسات عليا (ماجستير/دكتوراه)	88	20.8%
الإجمالي	424	100%

يتبين من الجدول أن نصف أفراد العينة (50.2%) يحملون درجة البكالوريوس، يليهم حملة الدراسات العليا بنسبة (20.8%)، ثم حملة الدبلوم بنسبة (16.7%)، وأخيراً حملة الثانوية العامة أو أقل بنسبة (12.3%). ويُشير هذا التوزيع إلى أن غالبية أفراد العينة (71.0%) يحملون مؤهلات جامعية أو أعلى، مما يُعزز من قدرتهم على فهم فقرات الاستبانة والإجابة عنها بدقة.

جدول (8): توزيع أفراد العينة وفقاً لمدة استخدام الخدمات المصرفية الإلكترونية

مدة الاستخدام	التكرار	النسبة المئوية
أقل من سنة	29	6.8%
من سنة إلى أقل من 3 سنوات	76	17.9%
من 3 سنوات إلى أقل من 5 سنوات	112	26.4%
من 5 سنوات إلى أقل من 10 سنوات	131	30.9%

17.9%	76	10 سنوات فأكثر
100%	424	الإجمالي

يُظهر الجدول أن الفئة الأكثر تمثيلاً هي فئة (من 5 إلى أقل من 10 سنوات) بنسبة (30.9%)، تليها فئة (من 3 إلى أقل من 5 سنوات) بنسبة (26.4%). ويدل ذلك على أن غالبية أفراد العينة (75.2%) يمتلكون خبرة تزيد عن ثلاث سنوات في استخدام الخدمات المصرفية الإلكترونية، مما يمنحهم القدرة على تقييم أبعاد الأمن السيبراني ومستوى ثقتهم في المعاملات الإلكترونية بشكل واقعي.

جدول (9): توزيع أفراد العينة وفقاً لمعدل تكرار الاستخدام

النسبة المئوية	التكرار	معدل الاستخدام
38.7%	164	يوميًا
32.5%	138	عدة مرات أسبوعياً
17.0%	72	مرة أسبوعياً
8.5%	36	عدة مرات شهرياً
3.3%	14	مرة شهرياً أو أقل
100%	424	الإجمالي

يتبين من الجدول أن النسبة الأكبر من أفراد العينة (38.7%) يستخدمون الخدمات المصرفية الإلكترونية بشكل يومي، يليهم من يستخدمونها عدة مرات أسبوعياً بنسبة (32.5%). ويدل ذلك على أن أكثر من سبعين بالمئة من أفراد العينة (71.2%) يُعدّون مستخدمين نشطين للخدمات المصرفية الإلكترونية، مما يُعزز من مصداقية استجاباتهم وارتباطها بتجارهم الفعلية.

2.4 التحليل الوصفي لمحاوَر الدراسة و أبعادها

تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على فقرات كل بُعد ومحور، وذلك لتحديد مستوى الموافقة وترتيب الفقرات والأبعاد وفقاً لأهميتها النسبية. وقد تمّ اعتماد المعيار التالي لتفسير المتوسطات الحسابية وفقاً لمقياس ليكرت الخماسي: من (1.00) إلى (1.80) منخفض جداً، من (1.81) إلى (2.60) منخفض، من (2.61) إلى (3.40) متوسط، من (3.41) إلى (4.20) مرتفع، من (4.21) إلى (5.00) مرتفع جداً.

التحليل الوصفي للمتغير المستقل: الأمن السيبراني

أ. البُعد الأول: سرية المعلومات

جدول (10): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد سرية المعلومات

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
1	يوفر المصرف أنظمة تشفير متقدمة لحماية بياناتي المالية أثناء تنفيذ المعاملات الإلكترونية	4.18	0.793	2	مرتفع
2	يتطلب المصرف إجراءات مصادقة متعددة العوامل للتحقق من هويتي قبل الوصول إلى حسابي	4.31	0.716	1	مرتفع جداً
3	أشعر بأن المصرف يمنع أي جهة غير مصرح لها من الاطلاع على بياناتي المصرفية	3.94	0.871	3	مرتفع

مرتفع	4	0.903	3.87	يُطبَّق المصرف سياسات صارمة تقصر الوصول إلى بياناتي على الموظفين المخوّلين فقط	4
مرتفع		0.692	4.08	المتوسط العام لُبُعد سرية المعلومات	

يتبيّن من الجدول أن المتوسط العام لُبُعد سرية المعلومات بلغ (4.08) بانحراف معياري (0.692) وبمستوى مرتفع. وقد جاءت الفقرة المتعلقة بإجراءات المصادقة المتعددة العوامل في الترتيب الأول بمتوسط حسابي (4.31)، بينما جاءت الفقرة المتعلقة بسياسات قصر الوصول على الموظفين المخوّلين في الترتيب الأخير بمتوسط (3.87). ويُشير ذلك إلى أن أفراد العينة يُدركون إجراءات المصادقة التقنية بدرجة أعلى من السياسات التنظيمية الداخلية التي قد لا تكون مرئية لهم بشكل مباشر.

ب. البُعد الثاني: سلامة النظام

جدول (11): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد سلامة النظام

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
5	يتم تنفيذ معاملاتي المصرفية الإلكترونية بدقة تامة دون أخطاء في المبالغ أو البيانات	4.11	0.814	2	مرتفع
6	يحتفظ النظام المصرفي الإلكتروني بسجلات دقيقة وكاملة لجميع معاملاتي	4.23	0.742	1	مرتفع جداً
7	لم أتعرض لأي تغيير غير مبرر في بيانات حسابي أو أرصدي عند استخدام الخدمات الإلكترونية	3.96	0.867	3	مرتفع

مرتفع	4	0.831	4.07	يُوقَّر المصرف آليات تُمكنني من التحقق من صحة معاملاتي فور تنفيذها عبر إشعارات فورية	8
-------	---	-------	------	--	---

|| المتوسط العام لُبُعد سلامة النظام || 0.714 | 4.09 | مرتفع |

يُظهر الجدول أن المتوسط العام لُبُعد سلامة النظام بلغ (4.09) بانحراف معياري (0.714) وبمستوى مرتفع. وقد تصدّرت الفقرة المتعلقة باحتفاظ النظام بسجلات دقيقة وكاملة للمعاملات الترتيب الأول بمتوسط (4.23)، بينما جاءت الفقرة المتعلقة بعدم التعرض لتغييرات غير مبررة في بيانات الحساب في الترتيب الثالث بمتوسط (3.96). ويعكس ذلك أن العملاء يُقدّرون وجود سجلات موثقة للمعاملات كمؤشر ملموس على سلامة النظام.

ج. البُعد الثالث: الموثوقية

جدول (12): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الموثوقية

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
9	تعمل الخدمات المصرفية الإلكترونية لمصرفي بشكل متواصل دون انقطاعات متكررة	3.89	0.886	3	مرتفع
10	أستطيع الوصول إلى حسابي وتنفيذ معاملاتي في أي وقت أحتاج إليه عبر القنوات الإلكترونية	4.14	0.768	1	مرتفع

11	يتعامل النظام المصرفي الإلكتروني بكفاءة مع أوقات الذروة دون تراجع ملحوظ في الأداء	3.78	0.921	4	مرتفع
12	في حال حدوث أي خلل تقني يتم معالجته بسرعة واستعادة الخدمة خلال وقت قصير	3.91	0.854	2	مرتفع
	المتوسط العام لبُعد الموثوقية	3.93	0.738		مرتفع

يتبين من الجدول أن المتوسط العام لبُعد الموثوقية بلغ (3.93) بانحراف معياري (0.738) وبمستوى مرتفع، وهو الأقل بين أبعاد الأمن السيبراني الأربعة. وقد جاءت الفقرة المتعلقة بإمكانية الوصول وتنفيذ المعاملات في أي وقت في الترتيب الأول بمتوسط (4.14)، بينما جاءت الفقرة المتعلقة بكفاءة الأداء في أوقات الذروة في الترتيب الأخير بمتوسط (3.78). ويُشير ذلك إلى أن أفراد العينة يرون أن الأنظمة المصرفية الإلكترونية متاحة بشكل عام لكنها قد تشهد تراجعاً في الأداء خلال فترات الاستخدام المكثف.

د. البُعد الرابع: الخصوصية

جدول (13): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الخصوصية

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
13	يلتزم المصرف بعدم مشاركة بياناتي الشخصية مع أطراف ثالثة دون الحصول على موافقتي المسبقة	3.97	0.862	2	مرتفع

14	يُوقَّر المصرف سياسة خصوصية واضحة ومفهومة تُبَيِّن كيفية جمع بياناتي واستخدامها	3.82	0.913	4	مرتفع
15	يُتيح لي المصرف إمكانية التحكم في إعدادات الخصوصية الخاصة بحسابي الإلكتروني	3.86	0.894	3	مرتفع
16	أثق بأن المصرف يستخدم بياناتي الشخصية فقط للأغراض التي جُمعت من أجلها	4.03	0.827	1	مرتفع
	المتوسط العام لبُعد الخصوصية	3.92	0.751		مرتفع

يُظهر الجدول أن المتوسط العام لبُعد الخصوصية بلغ (3.92) بانحراف معياري (0.751) وبمستوى مرتفع. وقد تصدّرت الفقرة المتعلقة بالثقة في استخدام البيانات للأغراض المحددة الترتيب الأول بمتوسط (4.03)، بينما جاءت الفقرة المتعلقة بوضوح سياسة الخصوصية في الترتيب الأخير بمتوسط (3.82). ويُشير ذلك إلى وجود فجوة بين ثقة العملاء العامة في نوايا المصرف وبين إدراكهم الفعلي لتفاصيل سياسات الخصوصية المعلنة.

هـ. ملخص التحليل الوصفي لأبعاد المتغير المستقل

جدول (14): ترتيب أبعاد الأمن السيبراني وفقاً للمتوسطات الحسابية

الترتيب	البُعد	المتوسط الحسابي	الانحراف المعياري	المستوى
1	سلامة النظام	4.09	0.714	مرتفع
2	سرية المعلومات	4.08	0.692	مرتفع
3	الموثوقية	3.93	0.738	مرتفع

مرتفع	0.751	3.92	الخصوصية	4
مرتفع	0.668	4.01	المتوسط العام للأمن السيبراني	

يتضح من الجدول أن المتوسط العام لمتغير الأمن السيبراني بلغ (4.01) بمستوى مرتفع، وأن بُعد سلامة النظام جاء في الترتيب الأول بمتوسط (4.09)، يليه بُعد سرية المعلومات بمتوسط (4.08)، ثم بُعد الموثوقية بمتوسط (3.93)، وأخيراً بُعد الخصوصية بمتوسط (3.92). ويُلاحظ تقارب المتوسطات بين الأبعاد الأربعة مما يعكس إدراكاً متوازناً نسبياً لدى العملاء لمختلف جوانب الأمن السيبراني في المصارف السعودية.

التحليل الوصفي للمتغير التابع: ثقة العملاء في المعاملات البنكية الإلكترونية

جدول (15): المتوسطات الحسابية والانحرافات المعيارية لفقرات محور ثقة العملاء

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
17	أشعر بالأمان عند تنفيذ معاملاتتي المالية عبر القنوات الإلكترونية لمصرفي	4.06	0.827	3	مرتفع
18	أثق بأن مصرفي قادر على حماية أموالتي من أي اختراق أو سرقة إلكترونية	3.94	0.876	6	مرتفع
19	أعتقد أن المعاملات المصرفية الإلكترونية آمنة بالقدر الكافي لتنفيذ جميع أنواع العمليات المالية	3.87	0.914	8	مرتفع
20	أفضل إجراء معاملاتتي المالية إلكترونياً لثقتي في أمان الأنظمة المصرفية الرقمية	4.12	0.783	2	مرتفع

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
21	أثق بأن المصرف سيُعوضني في حال تعرض حسابي لأي اختراق أو عملية غير مصرح بها	3.79	0.943	10	مرتفع
22	أشعر بالاطمئنان عند إدخال بياناتي الشخصية والمالية في المنصات الإلكترونية لمصرفي	3.98	0.851	5	مرتفع
23	أثق بأن أي خلل تقني في المعاملات الإلكترونية سيتم معالجته بشكل عادل وسريع	3.83	0.907	9	مرتفع
24	لا أتردد في تحويل مبالغ كبيرة عبر القنوات الإلكترونية لمصرفي	3.74	0.957	11	مرتفع
25	أوصي المقربين مني باستخدام الخدمات المصرفية الإلكترونية لمصرفي بناءً على ثقتي فيها	4.03	0.812	4	مرتفع
26	أشعر بأن مصرفي يبذل جهوداً كافية لتحديث أنظمتة الأمنية باستمرار	3.91	0.869	7	مرتفع
27	أثق بأن بياناتي المصرفية لن تُستخدم لأغراض لم أوافق عليها	3.89	0.882	8	مرتفع
28	بشكل عام أشعر بمستوى مرتفع من الثقة في أمان المعاملات البنكية الإلكترونية لمصرفي	4.16	0.764	1	مرتفع

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
	المتوسط العام لثقة العملاء	3.94	0.724		مرتفع

يتبين من الجدول أن المتوسط العام لمحور ثقة العملاء في المعاملات البنكية الإلكترونية بلغ (3.94) بانحراف معياري (0.724) وبمستوى مرتفع. وقد جاءت الفقرة (28) المتعلقة بالشعور العام بالثقة في أمان المعاملات في الترتيب الأول بمتوسط (4.16)، تلتها الفقرة (20) المتعلقة بتفضيل إجراء المعاملات إلكترونياً بمتوسط (4.12). في المقابل، جاءت الفقرة (24) المتعلقة بعدم التردد في تحويل مبالغ كبيرة في الترتيب الأخير بمتوسط (3.74). ويكشف هذا التباين عن أن الثقة العامة في أمان المعاملات مرتفعة لكنها تتراجع عندما يتعلق الأمر بقرارات مالية ذات مخاطرة أعلى كتحويل مبالغ كبيرة، مما يشير إلى أن الثقة ليست مطلقة بل تتدرج وفقاً لمستوى المخاطرة المدركة.

3.4 فرضيات الدراسة

اختبار الفرض الرئيس

"هناك أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) للأمن السيبراني بأبعاده المختلفة (سرية المعلومات، سلامة النظام، الموثوقية، الخصوصية) على ثقة العملاء في المعاملات البنكية الإلكترونية في المصارف السعودية".

للتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي المتعدد (Multiple Regression)

بهدف قياس تأثير أبعاد الأمن السيبراني (كمتغيرات مستقلة) على ثقة العملاء في المعاملات البنكية الإلكترونية (كمتغير تابع). وقد جاءت نتائج التحليل كما يلي:

جدول (16): نتائج تحليل الانحدار المتعدد لأثر أبعاد الأمن السيبراني على ثقة العملاء

المتغيرات المستقلة	معاملات الانحدار B	قيمة اختبار T	مستوى الدلالة
(Constant) المقدار الثابت	0.347	2.864	0.004**
سرية المعلومات	0.264	5.473	0.000**
سلامة النظام	0.218	4.316	0.000**
الموثوقية	0.312	6.127	0.000**
الخصوصية	0.179	3.642	0.000**
معامل الارتباط R = 0.842	معامل التحديد R ² = 0.709		
قيمة الاختبار F = 255.374	القيمة الاحتمالية = 0.000		

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

تُشير نتائج تحليل الانحدار المتعدد الموضحة في الجدول إلى وجود علاقة تأثيرية دالة إحصائياً بين أبعاد الأمن السيبراني كمتغيرات مستقلة وثقة العملاء في المعاملات البنكية الإلكترونية كمتغير تابع. فقد بلغ معامل التحديد (R^2) قيمة قدرها (0.709)، وهي نسبة مرتفعة تدل على أن (70.9%) من التباين في ثقة العملاء في المعاملات البنكية الإلكترونية يمكن تفسيره من خلال أبعاد الأمن السيبراني الأربعة مجتمعة. كما تُشير قيمة معامل الارتباط ($R = 0.842$) إلى وجود ارتباط قوي بين المتغيرات المدروسة. وقد بلغت قيمة اختبار (255.374) F بمستوى دلالة (0.000) وهي دالة إحصائياً عند مستوى (0.01) مما يؤكد معنوية النموذج ككل.

أما على مستوى الأبعاد الفردية، فقد تبين أن بُعد "الموثوقية" هو الأكثر تأثيراً على ثقة العملاء، حيث بلغ معامل الانحدار له ($B = 0.312$)، وبلغت قيمة T (6.127) بدلالة معنوية عالية. ($\text{Sig.} = 0.000$) ويؤكد ذلك الدور المحوري الذي يلعبه اتساق أداء الأنظمة المصرفية الإلكترونية ودقتها واستمراريتها في بناء ثقة العملاء وتعزيزها. كما جاء بُعد "سرية المعلومات" في الترتيب الثاني بمعامل انحدار ($B = 0.264$) وبدلالة

إحصائية عالية، يليه بُعد "سلامة النظام" بمعامل ($B = 0.218$) ، وأخيراً بُعد "الخصوصية" بمعامل ($B = 0.179$) وجميعها ذات دلالة إحصائية عند مستوى (0.01).

وبناءً على ذلك، تُؤكد هذه النتائج قبول الفرض الرئيس القائل بوجود أثر ذي دلالة إحصائية للأمن السيبراني بأبعاده المختلفة على ثقة العملاء في المعاملات البنكية الإلكترونية في المصارف السعودية.

اختبار الفرض الفرعي الأول

"هناك أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لسرية المعلومات على ثقة العملاء في التعاملات البنكية الإلكترونية".

للتحقق من صحة هذا الفرض تمّ استخدام تحليل الانحدار الخطي البسيط (Simple Linear Regression)، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (17): تحليل الانحدار الخطي البسيط لقياس أثر سرية المعلومات على ثقة العملاء

المعاملاتCoefficient				المتغير	ANOVAتحليل التباين				ملخص	المتغير
				المستقل					النموذج	التابع
Sig. t	T	الخطأ المعياري	B	سرية المعلومات	Sig. F	F المحسوبة	درجة الحرية df	معامل التحديد r ²	معامل الارتباط r	ثقة العملاء
0.000	20.883	0.036	0.746		0.000	436.127	1	0.508	0.713	

وللتحقق من هذه الفرضية، تمّ استخدام تحليل الانحدار الخطي البسيط لقياس تأثير "سرية المعلومات" باعتبارها أحد أبعاد الأمن السيبراني على "ثقة العملاء في التعاملات البنكية الإلكترونية". وقد جاءت النتائج الإحصائية كما هو موضح في الجدول (4-15)، حيث بلغ معامل الارتباط ($r = 0.713$) ، وهو

ما يعكس وجود علاقة ارتباط موجبة قوية بين المتغيرين. كما بلغت قيمة معامل التحديد ($R^2 = 0.508$) ، مما يشير إلى أن (50.8%) من التباين في ثقة العملاء يُمكن تفسيره من خلال متغير سرية المعلومات وحده.

وبالاطلاع على نتائج تحليل التباين (ANOVA) ، نجد أن قيمة F المحسوبة بلغت (436.127) بمستوى دلالة (Sig. = 0.000) ، وهي دالة إحصائياً عند مستوى (0.01) ، مما يُعزز من دلالة النموذج ككل في تفسير الفرضية. أما على مستوى معاملات الانحدار ، فقد بلغ معامل التأثير ($B = 0.746$) بقيمة ($T = 20.883$) وهي دالة عند مستوى (Sig. = 0.000) ، مما يدل على أن أي زيادة بمقدار وحدة واحدة في سرية المعلومات تؤدي إلى زيادة بمقدار (0.746) في مستوى ثقة العملاء في التعاملات البنكية الإلكترونية ضمن شروط النموذج.

وبناءً على ذلك ، يتم قبول الفرض الفرعي الأول القائل بوجود أثر ذي دلالة إحصائية لسرية المعلومات على ثقة العملاء في التعاملات البنكية الإلكترونية.

اختبار الفرض الفرعي الثاني

"هناك أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لسلامة النظام على إدراك العملاء لأمان المعاملات البنكية الإلكترونية".

للتحقق من صحة هذا الفرض تمّ استخدام تحليل الانحدار الخطي البسيط ، وجاءت النتائج كما يلي:

جدول (18): تحليل الانحدار الخطي البسيط لقياس أثر سلامة النظام على ثقة العملاء

المتغير	ملخص	المتغير
التابع	تحليل التباين ANOVA	المعاملات Coefficient
النموذج		المستقل

ثقة العملاء	معامل الارتباط	معامل التحديد	درجة الحرية	F المحسوبة	Sig. F	سلامة النظام	B	الخطأ المعياري	T	Sig. t
	r	r ²	df				0.692	0.036	19.164	0.000

تُشير النتائج الموضحة في الجدول إلى وجود علاقة ارتباط موجبة قوية بين سلامة النظام وثقة العملاء، حيث بلغ معامل الارتباط ($r = 0.682$) كما بلغت قيمة معامل التحديد ($R^2 = 0.465$) مما يعني أن 46.5% من التباين في ثقة العملاء يُمكن تفسيره من خلال متغير سلامة النظام منفرداً. وقد بلغت قيمة F المحسوبة (367.243) بمستوى دلالة ($\text{Sig.} = 0.000$) مما يؤكد معنوية النموذج. كما بلغ معامل الانحدار ($B = 0.692$) بقيمة ($T = 19.164$) وبدلالة إحصائية عالية، مما يدل على أن أي زيادة بمقدار وحدة واحدة في سلامة النظام تؤدي إلى زيادة بمقدار (0.692) في إدراك العملاء لأمان المعاملات البنكية الإلكترونية.

وبناءً على ذلك، يتم قبول الفرض الفرعي الثاني القائل بوجود أثر ذي دلالة إحصائية لسلامة النظام على إدراك العملاء لأمان المعاملات البنكية الإلكترونية.

اختبار الفرض الفرعي الثالث

"هناك أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) للموثوقية في بناء واستدامة ثقة العملاء في القنوات الرقمية البنكية".

للتحقق من صحة هذا الفرض تمّ استخدام تحليل الانحدار الخطي البسيط، وجاءت النتائج كما يلي:

الفصل الخامس: النتائج والتوصيات

1.5 نتائج الدراسة

1. النتائج المتعلقة بالفرضية الرئيسية

أظهرت نتائج تحليل الانحدار المتعدد وجود أثر ذي دلالة إحصائية لأبعاد الأمن السيبراني مجتمعةً على ثقة العملاء في المعاملات البنكية الإلكترونية، إذ بلغ معامل الارتباط المتعدد ($R = 0.842$) ومعامل التحديد ($R^2 = 0.709$)، مما يعني أن الأبعاد الأربعة للأمن السيبراني تُفسّر مجتمعةً ما يقارب 70.9% من التباين في مستوى ثقة العملاء. ويمكن تفسير هذه النتيجة بأن العميل المصرفي في البيئة الرقمية يبني ثقته على تقييم شامل ومتكامل لمنظومة الحماية التي يوفرها البنك، فلا يكفي أن يتحقق بُعد واحد من أبعاد الأمان بينما تظل الأبعاد الأخرى ضعيفة، بل إن إدراك العميل لتكامل هذه الأبعاد هو ما يولّد لديه الشعور بالأمان ويُعزز رغبته في الاستمرار باستخدام القنوات الإلكترونية. وتتسق هذه النتيجة مع ما توصلت إليه دراسة الهلسه والشيخ (2021) التي أكدت أن مقومات الأمن السيبراني بأبعادها المتعددة تؤثر تأثيراً جوهرياً في جودة المخرجات المؤسسية للبنوك التجارية، كما تتوافق مع دراسة زريقات والحوامده (2022) التي بيّنت أن حوكمة الأمن السيبراني بمكوناتها المتكاملة تسهم في تعزيز فعالية العمليات المصرفية الإلكترونية. وتؤيد هذه النتيجة أيضاً ما أشارت إليه دراسة حسين وأبو الغنم (2022) من أن التعامل مع الأمن السيبراني كمنظومة شاملة — لا كإجراءات تقنية مجزأة — هو ما يحمي سمعة البنوك ويرسخ مكانتها في أذهان العملاء.

كشفت نتائج تحليل الانحدار البسيط عن وجود أثر إيجابي ذي دلالة إحصائية لسرية المعلومات على ثقة العملاء، حيث بلغ معامل الارتباط ($r = 0.713$) ومعامل التحديد ($R^2 = 0.508$)، أي أن بُعد السرية وحده يُفسّر ما يزيد عن نصف التباين في ثقة العملاء. وتُعدّ هذه النتيجة منطقية في السياق المصرفي السعودي، إذ يتعامل العميل مع بيانات بالغة الحساسية تشمل أرصده المالية وتحويلات وبيانات هويته الشخصية، وأي إحساس بإمكانية تسرّب هذه البيانات أو وصول أطراف غير مخوّلة إليها يُقوّض ثقته

جذرًا في المنصة البنكية. كما أن البيئة السعودية تتميز بارتفاع الوعي المجتمعي تجاه خصوصية البيانات المالية، مما يجعل السرية مطلبًا جوهريًا وليس مجرد ميزة إضافية. وتتفق هذه النتيجة مع دراسة الغامدي والمصطفي (2021) التي أثبتت أن السرية تمثل البُعد الأكثر تأثيرًا في تحقيق الميزة التنافسية للمؤسسات، وكذلك مع دراسة عبد الفاتح (2022) التي أوضحت أن الوعي بسرية المعلومات يُعزز إدراك العملاء لمستوى الأمان المصرفي. كما تتوافق مع ما أكدته دراسة العبدالات والشورة (2023) من أن آليات حماية السرية في البنوك التجارية تُعد مدخلًا أساسيًا لبناء علاقة ثقة مستدامة مع العملاء في بيئة التسويق الإلكتروني.

بيّنت النتائج وجود أثر إيجابي ذي دلالة إحصائية لسلامة النظام على ثقة العملاء، بمعامل ارتباط بلغ $(r = 0.682)$ ومعامل تحديد $(R^2 = 0.465)$ ويمكن تفسير ذلك بأن العميل حين يُجري عملية تحويل مالي أو يطلع على كشف حسابه الإلكتروني يتوقع أن تكون البيانات المعروضة دقيقة وغير قابلة للتلاعب، فأى خلل في سلامة البيانات — كظهور مبلغ مختلف عن المحوّل أو تسجيل عملية لم يقم بها العميل — يُحدث صدمة فورية تُفضي إلى فقدان الثقة بصورة قد يصعب استعادتها. وعلى الرغم من أن هذا البُعد جاء في المرتبة الأخيرة من حيث قوة التأثير مقارنة بالأبعاد الأخرى، إلا أن ذلك لا يعني ضعف أهميته، بل يُرجّح أن العملاء يتعاملون مع سلامة النظام بوصفها شرطًا أساسيًا مسلّمًا به في البيئة المصرفية، فيما تتباين مستويات إدراكهم بدرجة أكبر للأبعاد الأخرى كالموثوقية والسرية. وتتقاطع هذه النتيجة مع دراسة الهلسه والشيخ (2021) التي أوضحت أن سلامة نظم المعلومات تنعكس مباشرة على جودة التقارير المحاسبية وموثوقيتها لدى أصحاب المصلحة، كما تتسق مع دراسة البوانه وصالح (2023) التي أكدت أن مخاطر المساس بسلامة البيانات تُعد من أبرز العوامل المثبطة لاستخدام البطاقات المصرفية في البنوك الإسلامية.

أظهرت النتائج أن الموثوقية هي البُعد الأكثر تأثيرًا في ثقة العملاء من بين أبعاد الأمن السيبراني الأربعة، حيث بلغ معامل الارتباط $(r = 0.729)$ ومعامل التحديد $(R^2 = 0.531)$ ، مما يعني أن الموثوقية وحدها تُفسّر أكثر من 53% من التباين في الثقة. ويُفسّر هذا التفوق بأن العميل يتفاعل يوميًا مع النظام المصرفي الإلكتروني من خلال تجربة الاستخدام المباشرة، فتوقّف الخدمة أو بطء الاستجابة أو حدوث أعطال متكررة هي أمور يلمسها العميل فورًا ويربطها تلقائيًا بمدى قدرة البنك على حماية أمواله ومعلوماته.

فالموثوقية ليست مجرد مسألة تقنية تتعلق بالخوادم والبنية التحتية، بل هي ترجمة عملية يومية للالتزام بالبنك تجاه عملائه. كما أن سوق الخدمات المصرفية الإلكترونية في المملكة العربية السعودية يشهد تنافسًا متصاعدًا بين البنوك التقليدية والبنوك الرقمية الجديدة، مما يجعل العميل أكثر حساسية لأي تراجع في مستوى الأداء ويدفعه للمقارنة المستمرة بين مقدمي الخدمة. وتتوافق هذه النتيجة مع ما توصلت إليه دراسة (Krishna et al. (2025 التي أثبتت أن الموثوقية التقنية تُشكل العمود الفقري لثقة العملاء في الخدمات الرقمية، كما تتسق مع دراسة (Amer and Al-Omar (2023 التي ربطت بين استمرارية عمل الأنظمة وبين تعزيز ثقة المستخدمين في بيئات التحول الرقمي. وتُعضد أيضًا ما أشارت إليه دراسة زريقات والحوامده (2022) من أن حوكمة الأمن السيبراني تعتمد في جوهرها على ضمان استقرار الأنظمة واستمراريتها كشرط لازم لفعالية التجارة الإلكترونية في البنوك.

أكدت النتائج وجود أثر إيجابي ذي دلالة إحصائية للخصوصية على ثقة العملاء، بمعامل ارتباط $(r = 0.697)$ ومعامل تحديد $(R^2 = 0.486)$ وتعكس هذه النتيجة تنامي وعي العملاء السعوديين بحقوقهم في التحكم ببياناتهم الشخصية، لا سيما بعد صدور نظام حماية البيانات الشخصية في المملكة العربية السعودية الذي أرسى إطارًا قانونيًا واضحًا لحماية خصوصية الأفراد في البيئة الرقمية. فالعمل أصبح أكثر إدراكًا لحقه في معرفة كيفية جمع بياناته وتخزينها ومعالجتها، وأي شعور بأن البنك يستخدم بياناته لأغراض غير مصرح بها — كالتسويق لأطراف ثالثة دون موافقة صريحة — يُضعف ثقته بصورة ملحوظة. كما أن انتشار حالات اختراق البيانات التي تتناولها وسائل الإعلام عالميًا قد رفع سقف توقعات العملاء تجاه ممارسات الخصوصية في مصارفهم. وتتفق هذه النتيجة مع دراسة (Sebihi et al. (2024 التي أكدت أن الخصوصية تُعد من أقوى المحددات المؤثرة في ثقة العملاء بالخدمات المالية الرقمية، كما تتسق مع دراسة عبد الفاتح (2022) التي بيّنت أن وعي العملاء بإجراءات حماية خصوصيتهم يرتبط ارتباطًا وثيقًا بمستوى ثقتهم في التعاملات المصرفية الإلكترونية. وتؤيد كذلك ما أشارت إليه دراسة الغامدي والمصطفي (2021) من أن الخصوصية تتفاعل مع بقية أبعاد الأمن السيبراني لتشكيل تصور شامل لدى المستخدمين حول مستوى الحماية المقدمة.

2. النتائج المتعلقة بالتحليل الوصفي

كشف التحليل الوصفي أن تصورات عملاء المصارف السعودية تجاه مستوى الأمن السيبراني جاءت مرتفعة بمتوسط عام بلغ (4.01) ، وأن بُعد سلامة النظام حصل على أعلى متوسط (4.09) يليه سرية المعلومات (4.08) ثم الموثوقية (3.93) فالخصوصية (3.92). ويُفسَّر تصدّر بُعد سلامة النظام بأن المصارف السعودية استثمرت بكثافة في البنية التقنية لضمان دقة العمليات وسلامتها، وأن العملاء يلمسون ذلك من خلال ندرة الأخطاء في المعاملات اليومية. أما حصول الخصوصية على أدنى متوسط — وإن كان مرتفعاً نسبياً — فقد يُعزى إلى أن بعض العملاء لا يزالون يشعرون بعدم الوضوح الكافي حول سياسات البنوك في معالجة بياناتهم الشخصية ومشاركتها. كما بلغ المتوسط العام لثقة العملاء (3.94) وهو مستوى مرتفع يعكس تقدم البيئة المصرفية السعودية في بناء منظومة أمان فعالة، لكنه في الوقت ذاته يترك مساحة للتحسين خاصة في ما يتعلق بثقة العملاء في إجراء التحويلات المالية الكبيرة إلكترونياً التي حصلت على أدنى متوسط (3.74)، مما يشير إلى أن الثقة في العمليات عالية القيمة لا تزال تحتاج إلى تعزيز إضافي.

2.5 التوصيات

في ضوء ما أسفرت عنه الدراسة من نتائج، يمكن تقديم التوصيات التالية:

- ينبغي للمصارف السعودية زيادة الاستثمار في أنظمة التشغيل المستمر والتعافي من الكوارث بما يضمن عدم انقطاع الخدمات الإلكترونية، نظراً لأن الموثوقية أثبتت أنها البُعد الأكثر تأثيراً في ثقة العملاء.
- يُوصى بأن تتبنى المصارف سياسات خصوصية واضحة ومبسّطة يستطيع العميل فهمها بسهولة، مع إتاحة أدوات تمنحه تحكماً فعلياً في بياناته الشخصية من حيث الوصول والمشاركة والحذف.
- من المهم أن تُطلق المصارف حملات توعوية دورية تُعرّف العملاء بآليات حماية حساباتهم وكيفية التعرف على محاولات الاحتيال، مما يُسهم في رفع مستوى الثقة العامة بالقنوات الإلكترونية.

- يُقترح تطوير مستويات إضافية من المصادقة والتأكيد لعمليات التحويل الكبيرة، مثل التحقق البيومتري أو إشعارات التأكيد الفورية، لتخفيف تردد العملاء في إجراء هذه العمليات إلكترونياً.
- يُوصى بأن يُدمج الأمن السيبراني ضمن الأهداف الاستراتيجية للمصرف وليس كوظيفة تقنية فحسب، بحيث تخضع قراراته لإشراف مجلس الإدارة وتُقاس مؤشرات ضمن بطاقة الأداء المتوازن.
- ينبغي للمصارف إجراء اختبارات اختراق دورية وتحديث أنظمة الحماية بما يتواءم مع أحدث المعايير الدولية مثل ISO 27001 ومتطلبات الهيئة الوطنية للأمن السيبراني.
- يُوصى بتوسيع برامج استقطاب وتطوير الكفاءات السعودية في مجال الأمن السيبراني، بما يتوافق مع توجهات رؤية المملكة 2030 في بناء اقتصاد معرفي وتعزيز المحتوى المحلي في القطاع التقني.
- تفعيل آليات التغذية الراجعة الأمنية: من المفيد إنشاء قنوات اتصال مخصصة تُتيح للعملاء الإبلاغ عن أي ملاحظات أو مخاوف أمنية بسهولة وسرعة، مع ضمان الاستجابة الفورية والشفافة لهذه البلاغات.
- يُوصى بتكثيف التنسيق بين المصارف السعودية والجهات التنظيمية كالبنك المركزي السعودي والهيئة الوطنية للأمن السيبراني لتبادل المعلومات حول التهديدات المستجدة واعتماد معايير حماية موحدة ترفع المستوى الأمني للقطاع المصرفي بأكمله.

Abstract

This study aims to examine the impact of cybersecurity, encompassing four dimensions — information confidentiality, system integrity, reliability, and privacy — on customer trust in electronic banking transactions at Saudi banks. The study adopted a descriptive-analytical approach and employed a questionnaire as the primary data collection instrument. A convenience random sample of 450 electronic banking customers was targeted, yielding 424 valid responses at a rate of 94.2%. Data were statistically analysed using SPSS, applying descriptive statistics, Pearson correlation coefficients, Cronbach's alpha, and simple and multiple linear regression. The findings revealed a statistically significant positive impact of the combined cybersecurity dimensions on customer trust at ($\alpha \leq 0.01$), with a coefficient of determination of ($R^2 = 0.709$). Reliability emerged as the most influential dimension, followed by information confidentiality, privacy, and system integrity respectively. The study recommends strengthening the infrastructure supporting the reliability of electronic banking systems, adopting more transparent privacy policies, and intensifying cybersecurity awareness programmes directed at customers.

Keywords: cybersecurity, information confidentiality, system integrity, reliability, privacy, customer trust, electronic banking transactions, Saudi banks.

المراجع

المراجع العربية

- 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>
- البواعنة، سهل محمد سودي، و الطالب، غسان سالم صالح. (2023). أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من <http://search.mandumah.com/Record/1461033>
- التوني، شريهان مصطفى محمد. (2023). أثر وعي العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني: دراسة ميدانية على البنوك الحكومية بمحافظة بورسعيد. مجلة التجارة والتمويل، ع4 ، 609 - 653. مسترجع من <http://search.mandumah.com/Record/1442825>
- 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>
- الحجايا، ميرفت محمد فلاح، و الحباشنة، عبادة يوسف عبدالله. (2023). أثر الثقافة التنظيمية على الأمن السيبراني في الحكومة الإلكترونية الأردنية: وزارة العدل أنموذجاً (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة. مسترجع من <http://search.mandumah.com/Record/1445798>

- حسين، رانيا موسى عبدالله، و أبو الغنم، خالد محمد. (2022). أثر الأمن السيبراني في سمعة البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة عمان العربية، عمان. مسترجع من

<http://search.mandumah.com/Record/1357067>

- الخروف، فادي جمال سلامة، و الشيخ، عماد يوسف أحمد أحمد. (2025). أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي: الدور المعدل لمتطلبات البنك المركزي لتدقيق شركات التكنولوجيا المالية في الأردن (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.

مسترجع من <http://search.mandumah.com/Record/1569393>

- زريقات، محمد رفيق محمد، و الحوامدة، ثروت محمد محمود. (2022). أثر حوكمة الأمن السيبراني على فعالية التجارة الإلكترونية العالمية في البنوك التجارية العاملة في الأردن (رسالة ماجستير غير منشورة). جامعة جرش، جرش. مسترجع من <http://search.mandumah.com/Record/1305442>

- سيد، ايمان مصطفى كمال، حسين، حنان، و المنيوي، عائشة مصطفى حسن. (2021). تأثير مزايا التعامل الدائم على ثقة عملاء شركات الطيران. المجلة العلمية للاقتصاد والتجارة، ع 2، 77 - 90.

مسترجع من <http://search.mandumah.com/Record/1178441>

- الشهراني، محمد سعد معيض آل زهير. (2024). أثر الكلمة المنطوقة على ثقة العملاء: دراسة تطبيقية في شركة الخطوط الجوية العربية السعودية خلال سنة 1444 هـ. مجلة العلوم الاقتصادية والإدارية والقانونية، مج 8، ع 6، 34 - 51. مسترجع من

<http://search.mandumah.com/Record/1478326>

- 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، مج 44، ع 2، 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، مج 37، 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>
- العبدلات، صدام عبدالله الكريم، و الشورة، محمد سليم خليف. (2023). أثر الأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من <http://search.mandumah.com/Record/1461296>
- علي، هيام عيد عطية محمد، دياب، محمد عبدالقادر، و عباس، حنان جابر حسن. (2023). أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني: دراسة ميدانية. الفكر المحاسبي، مج27، ع4 ، 71 - 120. مسترجع من <http://search.mandumah.com/Record/1435091>
- العوايشة، آلاء فراس شحادة، و القضاة، منذر عبدالكريم أحمد. (2022). المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني. مجلة جامعة عمان العربية للبحوث - سلسلة البحوث القانونية، مج4، ع2 ، 8 - 32. مسترجع من <http://search.mandumah.com/Record/1321914>
- الغامدي، عهود أحمد، و المستادي، ولاء عبدالله عبدالرحمن. (2021). دور الأمن السيبراني في تحقيق الميزة التنافسية: دراسة ميدانية على موظفي مطار الملك عبدالعزيز الدولي بجدة. مجلة العلوم الاقتصادية والإدارية والقانونية، مج5، ع9 ، 144 - 164. مسترجع من <http://search.mandumah.com/Record/1176003>
- 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>
- الفلاح، حسام محمد سليمان، النسور، مروان محمد عبد، و العربيات، أيمن عبدالهادي. (2023). أثر تطبيق معايير الأمن السيبراني على أداء شركات الاتصالات الأردنية (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1460405>

- فؤاد، كريم علاء الدين أحمد، و عراقات، آلاء طارق. (2021). Assessing Resistance to Accept Electronic Wallets in Egypt. مجلة العلوم الإقتصادية والإدارية والقانونية، مج5، ع18 ، 204 - 224. مسترجع من <http://search.mandumah.com/Record/1237269>
- القرني، ربهام مدحت محمد. (2025). ثقة العملاء في جودة الخدمات المقدمة من الجمعيات الأهلية. مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية، ع38 ، 181 - 262. مسترجع من <http://search.mandumah.com/Record/1575688>
- 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>
- النقودي، سوزي فاروق. (2024). أثر الأمن السيبراني على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية. مجلة البحوث المحاسبية، ع4 ، 169 - 216. مسترجع من <http://search.mandumah.com/Record/1532431>
- الهلسه، تامر عيسى فائق، و الشيخ، عماد يوسف أحمد أحمد. (2021). أثر مقومات الأمن السيبراني في خصائص المعلومات المحاسبية: الدور المعدل COBIT 2019: دراسة ميدانية في البنوك التجارية الأردنية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من <http://search.mandumah.com/Record/1265714>

- Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, 14(8).
- Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. *Information & computer security*, 31(5), 635-654.
- Harun, U., & Amalia, R. (2025). Cyber crime vs cyber security: implications for customer trust in e-banking at Indonesian Islamic banks. *Jurnal Ilmu Perbankan dan Keuangan Syariah*, 7(1), 35-54.
- Hira, M., Hafeez, K., & Yasen, 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>
- Krishna, B., Krishnan, S., & Sebastian, M. P. (2025). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. *Information Technology & People*, 38(2), 714-756.
- Mamadiyarov, Z., & Karshiev, D. (2024). Cybersecurity in digital banking: safeguarding customer trust in Uzbekistan. *American Journal of Corporate Management*, 1(2), 13-18.

- 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>
- 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>
- 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>

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس أثر الأمن السيبراني على ثقة العملاء في المعاملات

البنكية الإلكترونية دراسة ميدانية على المصارف السعودية

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول

منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم

بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً

أن جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا

البحث، وسوف أزودكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الشخصية

1- النوع الاجتماعي ☐ ذكر ☐ أنثى

2- العمر ☐ 25 سنة فأقل ☐ من 25 – 35 سنة

☐ 35 – 45 سنة ☐ من 45 سنة فأكثر

3- المؤهل العلمي ☐ ثانوية عامة أو أقل ☐ دبلوم

☐ بكالوريوس ☐ دراسات عليا

4- سنوات الخبرة ☐ سنة فأقل ☐ من سنة – 3 سنوات

☐ من 3 – 5 سنوات ☐ 5 – 10 سنوات

☐ 10 سنوات فأكثر

5- معدل تكرار الاستخدام

☐ يوميا ☐ عدة مرات أسبوعيا

☐ مرة أسبوعيا ☐ عدة مرات شهريا

☐ مرة شهريا أو أقل

ثانيا محاور الاستبيان

✿ المحور الأول: الأمن السيبراني ، ضع إشارة (√) في المربع المناسب لاختيارك:

معارض بشدة	معارض	محايد	أوافق	أوافق بشدة	البعد
1. سرية المعلومات					
					يوفر المصرف أنظمة تشفير متقدمة لحماية بياناتي المالية أثناء تنفيذ المعاملات الإلكترونية
					يتطلب المصرف إجراءات مصادقة متعددة العوامل للتحقق من هويتي قبل الوصول إلى حسابي
					أشعر بأن المصرف يمنع أي جهة غير مصرح لها من الاطلاع على بياناتي المصرفية
					يُطبق المصرف سياسات صارمة تقصر الوصول إلى بياناتي على الموظفين المخوّلين فقط
2. سلامة النظام					
					يتم تنفيذ معاملاتي المصرفية الإلكترونية بدقة تامة دون أخطاء في المبالغ أو البيانات
					يحتفظ النظام المصرفي الإلكتروني بسجلات دقيقة وكاملة لجميع معاملاتي
					لم أتعرض لأي تغيير غير مبرر في بيانات حسابي أو أرصدي عند استخدام الخدمات الإلكترونية

المعارض بشدة أوافق بشدة محايد أوافق معارض بشدة البعد				
				يُوفّر المصرف آليات تُمكنني من التحقق من صحة معاملاتي فور تنفيذها عبر إشعارات فورية
3. الموثوقية				
				تعمل الخدمات المصرفية الإلكترونية لمصرفي بشكل متواصل دون انقطاعات متكررة
				أستطيع الوصول إلى حسابي وتنفيذ معاملاتي في أي وقت أحتاج إليه عبر القنوات الإلكترونية
				يتعامل النظام المصرفي الإلكتروني بكفاءة مع أوقات الذروة دون تراجع ملحوظ في الأداء
				في حال حدوث أي خلل تقني يتم معالجته بسرعة واستعادة الخدمة خلال وقت قصير
4. الخصوصية				
				يلتزم المصرف بعدم مشاركة بياناتي الشخصية مع أطراف ثالثة دون الحصول على موافقتي المسبقة
				يُوفّر المصرف سياسة خصوصية واضحة ومفهومة تُبيّن كيفية جمع بياناتي واستخدامها
				يُتيح لي المصرف إمكانية التحكم في إعدادات الخصوصية الخاصة بحسابي الإلكتروني
				أثق بأن المصرف يستخدم بياناتي الشخصية فقط للأغراض التي جُمعت من أجلها

✿ المحور الثاني: ثقة العملاء في المعاملات البنكية الإلكترونية، ضع إشارة (✓) في المربع

المناسب لاختيارك:

معارض بشدة	معارض	محايد	أوافق	أوافق بشدة	البعد
					أشعر بالأمان عند تنفيذ معاملاتي المالية عبر القنوات الإلكترونية لمصرفي
					أثق بأن مصرفي قادر على حماية أموال من أي اختراق أو سرقة إلكترونية
					أعتقد أن المعاملات المصرفية الإلكترونية آمنة بالقدر الكافي لتنفيذ جميع أنواع العمليات المالية
					أفضل إجراء معاملاتي المالية إلكترونياً لثقتي في أمان الأنظمة المصرفية الرقمية
					أثق بأن المصرف سيُعوضني في حال تعرض حسابي لأي اختراق أو عملية غير مصرح بها
					أشعر بالاطمئنان عند إدخال بياناتي الشخصية والمالية في المنصات الإلكترونية لمصرفي
					أثق بأن أي خلل تقني في المعاملات الإلكترونية سيتم معالجته بشكل عادل وسريع
					لا أتردد في تحويل مبالغ كبيرة عبر القنوات الإلكترونية لمصرفي

البعد					أوافق بشدة	أوافق	محايد	معارض	معارض بشدة
أوصي المقربين مني باستخدام الخدمات المصرفية الإلكترونية لمصرفي بناءً على ثقتي فيها									
أشعر بأن مصرفي يبذل جهوداً كافية لتحديث أنظمتة الأمنية باستمرار									
أثق بأن بياناتي المصرفية لن تُستخدم لأغراض لم أوافق عليها									
بشكل عام أشعر بمستوى مرتفع من الثقة في أمان المعاملات البنكية الإلكترونية لمصرفي									

مع خالص التقدير والاحترام

Mid Ocean University

College of Management



Master of business administration

The Impact of Cybersecurity on Customer Trust in Electronic Banking Transactions: A Field Study on Saudi Banks

Prepared by:

Supervision:

Dr. Al-Faisal Abdelhamid Mohamed Hassan

Dr. Fayez Jarad

1447-2026