الجمهورية العربية السورية
وزارة التعليم العالي والبحث العلمي
المعهد العالي لإدارة الأعمال

HIGHER INSTITUTE OF BUSINESS ADMINISTRATION

التسويق الأمني كأداة لتعزيز تبني تطبيقات الدفع الإلكتروني في سوريا

Security marketing as a tool to promote adoption of e-payment applications in Syria

رسالة أعدّت لنيل درجة الماجستير في إدارة الأعمال

اختصاص: إدارة التسويق

إعداد الطالبة:

لجين يوسف البدوي

إشراف الدكتور:

حيّان ديب

العام الدراسي: 2024 – 2025

شكر وتقدير

أتوجه بأسمى آيات الشكر والتقدير والعرفان إلى الدكتور **حيّان ديب**، مشرفي الكريم، الذي تفضل بقبول الإشراف على هذه الرسالة، وأمدّني بتوجيهاته القيّمة وملاحظاته البنّاءة.

كما أتوجه بالشكر الجزيل إلى أعضاء لجنة المناقشة الكرام، الذين تفضلوا بقراءة هذه الرسالة بعناية فائقة لتقديم ملاحظاتهم الدقيقة و آراؤهم الغنيّة.

و أتقدم بخالص شكري وتقديري إلى جميع الدكاترة والأساتذة الأكارم في المعهد العالي لإدارة الأعمال، الذين أثروا مساري العلمي بمحاضراتهم المتميزة وخبراتهم الغنية.

كما أتوجه بشكري إلى إدارة المعهد العالي لإدارة الأعمال على توفيرها البيئة الأكاديمية المحفزة والإمكانيات اللازمة لإتمام هذا البحث. الشكر يمتد أيضاً إلى جميع الموظفين والكادر الإداري الذين ساهموا بطريقة مباشرة أو غير مباشرة في تذليل الصعوبات الإدارية واللوجستية.

الإهداء

إلى من كان دافعي وسندي في هذه الرحلة، إلى من كان الطريق معه أجمل وأكثر متعة.

إلى رفيق الروح: المهندس **عمّار مللي**.

إلى أهلي وأصدقائي وزملاء العمل، وكل من ساعدني ومدّ يد العون والتشجيع خلال رحلتي.

ملخص

لاحظ الباحث خلال عمله في قطاع التكنولوجيا السوري أن معظم الشركات السورية العاملة في مجال تطبيقات الدفع الإلكتروني تتغافل عن الحديث عن الأمان بشكل مباشر وحقيقي في حملاتها التسويقية. فبينما تركز شركات عالمية على إبراز الإجراءات الأمنية والثقة في رسائلها التسويقية، تفضل الشركات السورية التركيز على الميزات العملية (السرعة، السهولة، التوفر) دون إعطاء أمان البيانات والأموال الأولوية الكافية. تستهدف هذه الرسالة تحليل بعض العوامل المؤثرة على تبنّي تطبيقات الدفع الإلكتروني في السوق السوري، مع استخدام تطبيقMTN Cash كحالة عملية. تتمحور المشكلة الرئيسية حول صعوبة شركات التكنولوجيا في بناء ثقة العملاء وزيادة معدلات التبنّي. تتبنى الدراسة منهجية مدمجة تجمع بين البيانات الكمية (186 مستجيب) والنوعية (28 مشارك في مجموعات تركيز)، مما يوفر فهماً شاملاً للديناميكيات السلوكية. تستند الدراسة إلى نماذج تقبل التكنولوجيا (TAM, UTAUT) ونظرية الثقة، وتختبر ستة فرضيات تربط بين الأمان المدرك، الحملات التسويقية، تعقيد الإجراءات، الثقة، والتبنّي. أبرز النتائج تكمن في أن الثقة تمثل المحدد الأقوى للتبنّي (تفسّر 48٪ من التباين)، وتؤدي دوراً وسيطاً حاسماً بين العوامل الأخرى والتبنّي، بينما يعمل الأمان والحملات التسويقية بشكل أساسي عبر بناء هذه الثقة. تقدم الرسالة توصيات تسويقية عملية لتعزيز الأمان، بناء الثقة، وإعداد حملات مخصصة للفئات العمرية، مما يشكّل إطاراً استراتيجياً لزيادة التبنّي في الأسواق الناشئة.

الكلمات المفتاحية: التسويق الرقمي، التبنّي التكنولوجي، الثقة، الأمان المدرك، تطبيقات الدفع الإلكتروني، السوق السوري، حملات التسويق الأمنية، تعقيد الإجراءات.

Abstract

During her work in the Syrian technology sector, the researcher observed that most Syrian companies operating in the field of e-payment applications do not talk about security directly and genuinely in their marketing campaigns. While international companies focus on highlighting security measures and trust in their marketing messages, Syrian companies prefer to focus on practical features (speed, ease, availability) without giving sufficient priority to data and money security. This thesis aims to analyze some factors influencing the adoption of e-payment applications in the Syrian market, using MTN Cash as a case study. The main issue revolves around the difficulty of technological companies in building customer trust and increasing adoption rates. The study adopts a combined methodology that combines quantitative (186 respondents) and qualitative (28 participants in focus groups) data, providing a comprehensive understanding of behavioral dynamics. The study draws on technology acceptance models (TAM, UTAUT) and trust theory, and tests six hypotheses linking perceived security, marketing campaigns, procedural complexity, trust, and adoption. Key findings are that trust is the strongest determinant of adoption (explaining 48% of the variance) and plays a critical mediating role between other factors and adoption, while perceived security and marketing campaigns act primarily through trust. The thesis provides practical marketing recommendations to enhance security, build trust, and develop age-specific campaigns, forming a strategic framework to increase adoption in emerging markets.

Keywords: digital marketing, technology adoption, trust, perceived security, e-commerce applications, Syrian market, security marketing campaigns, procedural complexity.

الفهرس

فهرس الجداول

فهرس الأشكال

الفصل التمهيدي

الإطار العام للبحث

1. المقدمة والسياق الاستراتيجي

1.1 الوضع الراهن للسوق السوري

يمثل السوق السوري للخدمات المالية الرقمية فرصة كبيرة وتحدياً استراتيجياً في الوقت ذاته. بينما ينمو الطلب على حلول الدفع الإلكتروني نظراً للأوضاع الاقتصادية الحالية, فقد وجد الباحث من خلال خبرته و مجال عمله في شركة MTN ومشاركته في مشروع بناء تطبيق الدفع الإلكتروني MTN Cash أن الشركات العاملة في هذا القطاع تواجه معضلة حقيقية: كيفية الموازنة بين توفير خدمات آمنة وبسيطة الاستخدام في الوقت ذاته؟ وكيفية توصيل قيمة الأمان والموثوقية للعملاء من خلال حملات تسويقية فعالة؟.

تركز هذه الرسالة على تطبيق MTN Cash كدراسة حالة عملية، حيث يمثل هذا التطبيق نموذجاً قابلاً للتعميم على قطاع الدفع الرقمي بأكمله في السوق السوري.

1.2 الفرصة الاستراتيجية والحاجة للبحث

على الرغم من أهمية خدمات الدفع الإلكتروني، لا توجد دراسات محلية تربط بشكل شامل بين:

- مستوى الأمان المدرك

- فعالية الحملات التسويقية الأمنية
- مستوى ثقة العملاء
- القرار الفعلي بتبني التطبيق
- تجارب المستخدمين الحقيقية ودوافعهم الكامنة

هذا الفهم المتكامل ضروري لصناع القرار في الشركات لتحسين استراتيجياتهم التسويقية وتخصيص الموارد بكفاءة.

1.3 الأهمية التطبيقية (التسويقية)

- توصيات قابلة للتنفيذ: تقديم خطة عمل تسويقية محددة بالجداول الزمنية
- تقسيم السوق: تحديد الفئات المستهدفة واستراتيجيات التواصل المناسبة لكل فئة
- رؤى المستخدمين: الحصول على اقتراحات مباشرة من المستخدمين لتحسين التطبيق والحملات

2. تعريف المشكلة والأهداف

2.1 المشكلة الأساسية

التحدي الاستراتيجي الرئيسي:

كيف يمكن لشركة MTN (والشركات المشابهة) تحسين استراتيجياتها التسويقية لزيادة معدلات تبني تطبيق MTN Cash وبناء ثقة عملاء مستدامة في بيئة السوق السوري الحالية؟ ومادور أمان التطبيق؟

2.2 الأسئلة الحاسمة

1. ما مستوى إدراك العملاء لأمان التطبيق؟ وكيف يؤثر هذا الإدراك على قرارهم بالتبني؟
2. أي الفئات العمرية تحتاج حملات تسويقية مخصصة؟ وما الرسائل الأكثر فعالية؟
3. هل الحملات التسويقية الحالية فعالة؟ وهل تختلف فعاليتها حسب الفئات العمرية المستهدفة؟
4. هل تعقيد الإجراءات الأمنية يعيق التبني؟ وما درجة التعقيد المقبولة من وجهة نظر المستخدمين؟
5. ما دور الثقة كعامل وسيط في العملية الشرائية؟ وكيف يمكن تعزيزها؟
6. ما التجارب الحقيقية للمستخدمين؟ وما الاقتراحات المباشرة لتحسين التطبيق؟

3. أهداف الدراسة

3.1 الهدف الرئيسي

تطوير إطار تسويقي استراتيجي متكامل لتعزيز تبني تطبيقات الدفع الإلكتروني في السوق السوري، من خلال فهم العلاقة بين الأمان المدرك والثقة والحملات التسويقية وقرار التبني.

3.2 الأهداف الفرعية

الهدف	الطبيعة	المخرج المتوقع
قياس مستوى الأمان المدرك والثقة والتبني	كمي	متوسطات ومعاملات ارتباط
تحديد العلاقات السببية بين المتغيرات	كمي	نموذج انحدار ووساطة
فهم تجارب المستخدمين الحقيقية	نوعي	رؤى وقصص واقتباسات
تحديد الفروقات بين الفئات العمرية	مقارن	استراتيجيات مخصصة
استخلاص اقتراحات التحسين	نوعي	توصيات من المستخدمين
تطوير توصيات تسويقية قابلة للتنفيذ	تطبيقي	خطة عمل مرحلية

جدول 1 الأهداف الفرعية للدراسة

4. متغيرات الدراسة

4.1 المتغيرات المستقلة

أ) الأمان المدرك (Perceived Security)

التعريف الإجرائي: الدرجة التي يشعر فيها مستخدم تطبيق MTN Cash بأن بياناته الشخصية والمالية محمية من الاختراق أو الاحتيال أو الاستخدام غير المصرح به.

الأبعاد:

- حماية البيانات الشخصية
- الإشعارات الفورية عند العمليات
- رمز التحقق والمصادقة الثنائية
- الحماية من الاحتيال

القياس: 4 عبارات بمقياس ليكرت الخماسي (الأسئلة 5–8 في الاستبانة)

ب) الحملات التسويقية الأمنية (Security Marketing Campaigns)

التعريف الإجرائي: مدى إدراك المستخدم للجهود التسويقية التي تبذلها الشركة المشغلة للتطبيق في توصيل رسائل الأمان والموثوقية، وتأثير هذه الحملات على شعوره بالطمأنينة.

الأبعاد:

- المعلومات الدورية عن عوامل الأمان
- الإعلانات المطمئنة
- المحتوى التعليمي عن الأمان

- الرسائل التسويقية المحفزة

القياس: 4 عبارات بمقياس ليكرت الخماسي (الأسئلة 9–12 في الاستبانة)

ج) تعقيد الإجراءات الأمنية (Security Procedures Complexity)

التعريف الإجرائي: الدرجة التي يشعر فيها المستخدم بأن إجراءات الأمان في التطبيق (مثل رموز التحقق وخطوات المصادقة) تُشكّل عبئاً أو تُبطئ إتمام المعاملات.

الأبعاد:

- سهولة الدخول للتطبيق (تم عكسه)
- كثرة خطوات الأمان
- بطء المعاملات بسبب التحقق
- انخفاض الراحة في الاستخدام

القياس: 4 عبارات بمقياس ليكرت الخماسي (الأسئلة 13–16 في الاستبانة)

ملاحظة :يُتوقع أن يكون تأثير هذا المتغير سلبياً على التبني.

4.2 المتغير الوسيط

ثقة العملاء (Customer Trust)

التعريف الإجرائي:مستوى الاطمئنان والاعتماد الذي يشعر به المستخدم تجاه تطبيق MTN Cash والشركة المشغلة له، واعتقاده بأن التطبيق سيحمي أمواله ومعلوماته.

الأبعاد:

- الاطمئنان عند إجراء المدفوعات
- الثقة بحماية الأموال والمعلومات
- الثقة بالتزام الشركة بتأمين البيانات
- المقارنة بالطرق التقليدية

القياس 4 :عبارات بمقياس ليكرت الخماسي (الأسئلة 17–20 في الاستبانة)

الدور الوسيط: التأثير غير المباشر عبر الثقة (الأمان المدرك ← الثقة ← التبني)

4.3 المتغير التابع

تبني التطبيق (App Adoption)

التعريف الإجرائي: القرار الفعلي باستخدام تطبيق MTN Cash بشكل منتظم ومستمر، والاستعداد للتوصية به للآخرين وتفضيله على البدائل المتاحة.

الأبعاد:

- الاستخدام المتكرر

- التوصية للآخرين
- نية الاستمرار في الاستخدام
- التفضيل على التطبيقات المنافسة

القياس: 4 عبارات بمقياس ليكرت الخماسي (الأسئلة 21–24 في الاستبانة)

4.4 المتغيرات الديموغرافية

المتغير	التصنيف	الهدف من قياسه
الجنس	ذكر / أنثى	فحص الفروقات في الإدراك والسلوك
العمر	5فئات (أقل من 20 حتى 50+)	تحديد الفئات المستهدفة للحملات
المستوى التعليمي	4مستويات	فهم علاقة التعليم بالتبني
الاستخدام السابق	نعم / لا	التحقق من الخبرة الفعلية

جدول 2 المتغيرات الديموغرافية

5. مجتمع الدراسة وعينتها

5.1 مجتمع الدراسة

التعريف:

يتكون مجتمع الدراسة من جميع مستخدمي تطبيق MTN Cash في الجمهورية العربية السورية، والذين يستخدمون التطبيق لإجراء المعاملات المالية الإلكترونية.

خصائص المجتمع:

- مستخدمون فعليون للتطبيق (ليسوا مستخدمين محتملين فقط)
- تنوع في الخصائص الديموغرافية (العمر، الجنس، التعليم، الموقع الجغرافي)
- مستويات متفاوتة من الخبرة والاستخدام

5.2 عينة الدراسة

أ) العينة الكمية (الاستبانة الالكترونية)

طريقة المعاينة :عينة ملائمة مع مراعاة التنوع الديموغرافي.

ب) العينة النوعية (مجموعات التركيز)

طريقة المعاينة :عينة هادفة لضمان تمثيل الفئات العمرية المختلفة.

6. فترة الدراسة

6.1 الجدول الزمني للدراسة

المرحلة	الفترة	المدة	المخرجات
الدراسات السابقة	أيار	4 أسابيع	مراجعة دراسات سابقة مشابهة
الإعداد والتخطيط	حزيران	4 أسابيع	خطة البحث، الإطار النظري الأولي
مراجعة الأدبيات	تموز	4 أسابيع	الإطار النظري الكامل
تطوير الأدوات	آب	أسبوعان	الاستبانة، دليل مجموعات التركيز
تجربة الاستبانة	آب	أسبوعان	تعديل صيغة أسئلة الاستبانة
تحكيم الاستبانة	أيلول	1 يوم	أخذ الموافقة من الدكتور المشرف
جمع البيانات الكمية	أيلول – تشرين الأول	8 أسابيع	186استجابة
جمع البيانات النوعية	تشرين الثاني	1 أسبوع	4جلسات، 28 مشارك

المرحلة	الفترة	المدة	المخرجات
تحليل البيانات	تشرين الثاني	2 أسبوع	النتائج الإحصائية والنوعية
كتابة التقرير	تشرين الثاني	1 أسبوع	الرسالة النهائية

جدول 3 الجدول الزمني للدراسة

6.2 حدود الدراسة

الحدود الموضوعية

تقتصر الدراسة على دراسة العلاقة بين:

- الأمان المدرك
- الحملات التسويقية الأمنية
- تعقيد الإجراءات الأمنية
- ثقة العملاء
- تبني التطبيق

ولا تتناول متغيرات أخرى مثل: السعر، جودة الخدمة، المنافسة، البنية التحتية.

الحدود المكانية

النطاق الجغرافي :الجمهورية العربية السورية

الحدود الزمانية

فترة جمع البيانات :أيلول – تشرين الثاني 2025

الحدود البشرية

- الفئة المستهدفة :مستخدمو تطبيق MTN Cash الفعليون فقط
- الاستثناء :المستخدمون المحتملون الذين لم يجربوا التطبيق

7. الدراسات السابقة

- إدراك الأمان والثقة والتبني: أجرى Almaiah وآخرون (2022) دراسة شاملة على تطبيقات الدفع الرقمية في السياق السعودي، حيث كشفت نتائجهم عن وجود علاقة ارتباط قوية جداً بين أمان التطبيق والثقة، وتأثير مباشر للثقة على التبني، مما يؤكد على الدور الوسيط للثقة في العلاقة بين الأمان والتبني. وقد استخدم الباحثون نموذج قياس مماثلاً يتضمن أربع بنود لقياس الأمان مع مقياس ليكرت الخماسي، وهو ما يتوافق مع المنهجية المعتمدة في الدراسة الراهنة.
- الحملات التسويقية ودورها في التبني: بحثت دراسة Kapoor و Sindwani (2021) في الهند تأثير الحملات التسويقية والعروض الترويجية على تبني المحافظ الإلكترونية، وأظهرت النتائج أن الحملات التسويقية التي تبرز جوانب الأمان لها تأثير إيجابي معنوي على نية التبني، خاصة لدى

الفئات الشابة. وتُشير هذه الدراسة إلى أهمية استهداف الفئات العمرية المختلفة بحملات متناسبة، وهو ما يتطابق مع أحد أهداف الدراسة الحالية.

- تعقيد الإجراءات الأمنية وتأثيره السلبي على الاستخدام: وجدت دراسة Hossain (2021) أن "مستويات التعقيد المتوسطة تسهم في تقليل مقاومة المستخدمين للتبني، بينما التعقيد الشديد يعتبر عائقاً كبيراً على الاستخدام المستمر" وهذا يعكس التوازن الدقيق الذي تسعى الدراسة الراهنة إلى فهمه بين الحماية الأمنية والراحة في الاستخدام.
- الدور الوسيط للثقة: قام Stewart وJörjens (2018) بفحص العلاقات المعقدة بين الأمان والثقة والتبني في سياق التكنولوجيا المالية في أوروبا. أوضحت نتائجهم أن الثقة تعمل كمتغير وسيط رئيسي يربط إدراك الأمان بنية التبني الفعلي. وقد دعمت دراسة Siagian وآخرون (2022) في السياق الإندونيسي هذه النتيجة، حيث أكدوا على أن الثقة والأمان يعتبران من أقوى محددات التبني الفعلي.
- الفروق الديموغرافية (وخاصة الجنس): كشفت دراسة Eksteen و Humbani (2021) في جنوب أفريقيا عن وجود فروق بين الجنسين في إدراك المخاطر والثقة في تطبيقات الدفع المحمول، مما يشير إلى أن العوامل الثقافية والسياقية قد تؤثر على هذه العلاقات. إلا أن هذه النتيجة لم تكن متسقة في جميع البيئات الجغرافية، مما يبرر الحاجة لدراسات محلية تتناول هذا الجانب في السياق السوري.

الفصل الأول

مراجعة الأدبيات النظرية

مقدمة القسم النظري

يستعرض هذا القسم الأساس النظري والمفاهيمي الذي تستند إليه الدراسة في فهم العوامل المؤثرة على تبنّي تطبيقات الدفع الإلكتروني. يبدأ بتحليل نماذج تقبل التكنولوجيا الرئيسية (TAM, UTAUT, UTAUT2) التي تشرح كيف يقبل المستخدمون التقنيات الحديثة من خلال عوامل مثل الفائدة المدركة وسهولة الاستخدام والتأثير الاجتماعي. ومن ثم ينتقل إلى نظريات الثقة في البيئة الرقمية، حيث يعرّف الثقة في البيئة الرقمية ويشرح مكوناتها، ويشرح أبعاد الثقة في تطبيقات الدفع (الثقة في التكنولوجيا، المؤسسة، الإطار التنظيمي). ومن ثم ينتقل إلى الأمن السيبراني والتسويق الرقمي حيث يشرح مفهوم الأمن السيراني وأهميته في التسويق الرقمي. و من ثم يستفيض في استراتيجيات التسويق الرقمي في القطاع المالي حيث يذكر أسسه ويشرح معنى التسويق الأمني ويذكر الحملات التوعوية والتسويقية والإعلانات بالتسويق الأمني. نهايةً، يأتي على ذكر تجربة المستخدم في التطبيقات المالية ويذكر أهمية التوازن بين الأمان وسهولة الاستخدام.

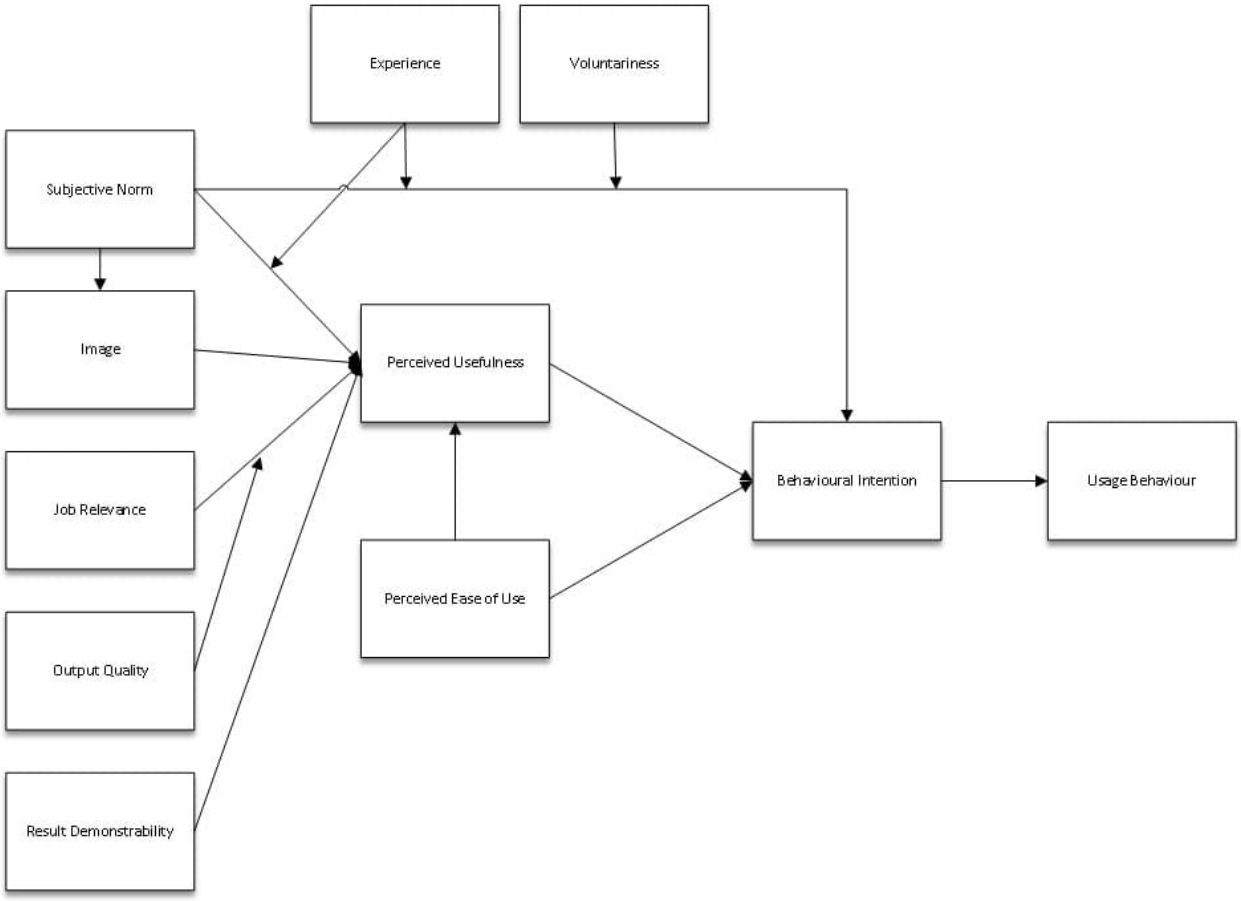
1. الأطر النظرية لتبني التكنولوجيا المالية الرقمية

1.1 نماذج قبول واستخدام التكنولوجيا

1.1.1 نموذج قبول التكنولوجيا (Technology Acceptance Model – TAM)

يُعد نموذج قبول التكنولوجيا (Technology Acceptance Model – TAM) أحد الأطر النظرية الأكثر تأثيراً في تفسير كيفية قبول المستخدمين للتقنيات الحديثة واستخدامها. طوّر ديفيس هذا النموذج في أواخر الثمانينيات استجابةً للمخاوف المتعلقة بمقاومة الأفراد للتكنولوجيا والفشل المتكرر للأنظمة الجديدة في تحقيق أهدافها .(Davis, 1989) يفترض النموذج أن قبول التكنولوجيا يُحدَّد بشكل أساسي من خلال عاملين رئيسيين: سهولة الاستخدام المدركة (Perceived Ease of Use) والفائدة المدركة (Perceived Usefulness) .(Venkatesh, 2000)

تشير سهولة الاستخدام المدركة إلى الدرجة التي يعتقد بها المستخدمون المحتملون أن استخدام تقنية معينة سيكون خالياً من الجهد، بينما تعكس الفائدة المدركة اعتقاد المستخدمين بأن استخدام التقنية سيعزز أداءهم في إنجاز المهام المطلوبة (Daviset al., 1989). وفقاً للنموذج، تؤثر هذه التصورات مباشرةً على الاتجاه نحو استخدام التكنولوجيا، والذي بدوره يشكل النية السلوكية للاستخدام، وصولاً إلى الاستخدام الفعلي للنظام .(Ajzen, 2011; Davis, 1993)



الشكل 1 نموذج قبول التكنولوجيا (TAM)

على مدار العقود الماضية، حظي نموذج TAM بقبول واسع كأداة فعالة للتنبؤ بقبول الأفراد للتقنيات الناشئة في مختلف السياقات (Ajibade, 2018). أثبتت الدراسات التطبيقية أن النموذج يتمتع بقوة تنبؤية عالية في تفسير سلوك المستخدمين تجاه مجموعة واسعة من التطبيقات التقنية، بما في ذلك التطبيقات المصرفية عبر الهاتف المحمول والخدمات المالية الرقمية (Granić, 2022). وقد أشارت مراجعة نقدية للنموذج إلى أن

TAM قد تطور عبر ثلاث مراحل رئيسية: مرحلة التبني، ومرحلة التحقق من الصحة، ومرحلة التوسع والتطوير (Han, 2003).

المرحلة	الفترة الزمنية	الخصائص الرئيسية	المتغيرات الأساسية
TAM الأصلي	1986–1989	التركيز على المتغيرات الأساسية	سهولة الاستخدام المدركة، الفائدة المدركة
TAM2	2000	إضافة العوامل الاجتماعية والمعرفية	المعايير الذاتية، الصورة، الجودة المدركة
TAM3	2008	دمج محددات سهولة الاستخدام والفائدة	الفعالية الذاتية، القلق من الحاسوب، التمتع المدرك

جدول 4 مراحل تطور نموذج قبول التكنولوجيا

مع ذلك، فقد واجه النموذج بعض الانتقادات المتعلقة بإفراطه في التبسيط وعدم أخذه في الاعتبار العوامل السياقية والاجتماعية المعقدة التي تؤثر على قبول التكنولوجيا (Ajibade, 2018). استجابةً لهذه الانتقادات، قام الباحثون بتطوير نسخ موسعة من النموذج، مثل TAM2 وTAM3، التي تدمج متغيرات إضافية مثل المعايير الذاتية، والخبرة السابقة، والطوعية في الاستخدام (Venkatesh & Bala, 2008). في سياق الخدمات المالية الرقمية، أثبتت النسخ الموسعة من TAM فعاليتها في تفسير العوامل المؤثرة على تبني تطبيقات

الدفع الإلكتروني، حيث تلعب الثقة والأمان دوراً محورياً إلى جانب سهولة الاستخدام والفائدة المدركة (Worthington, 2021).

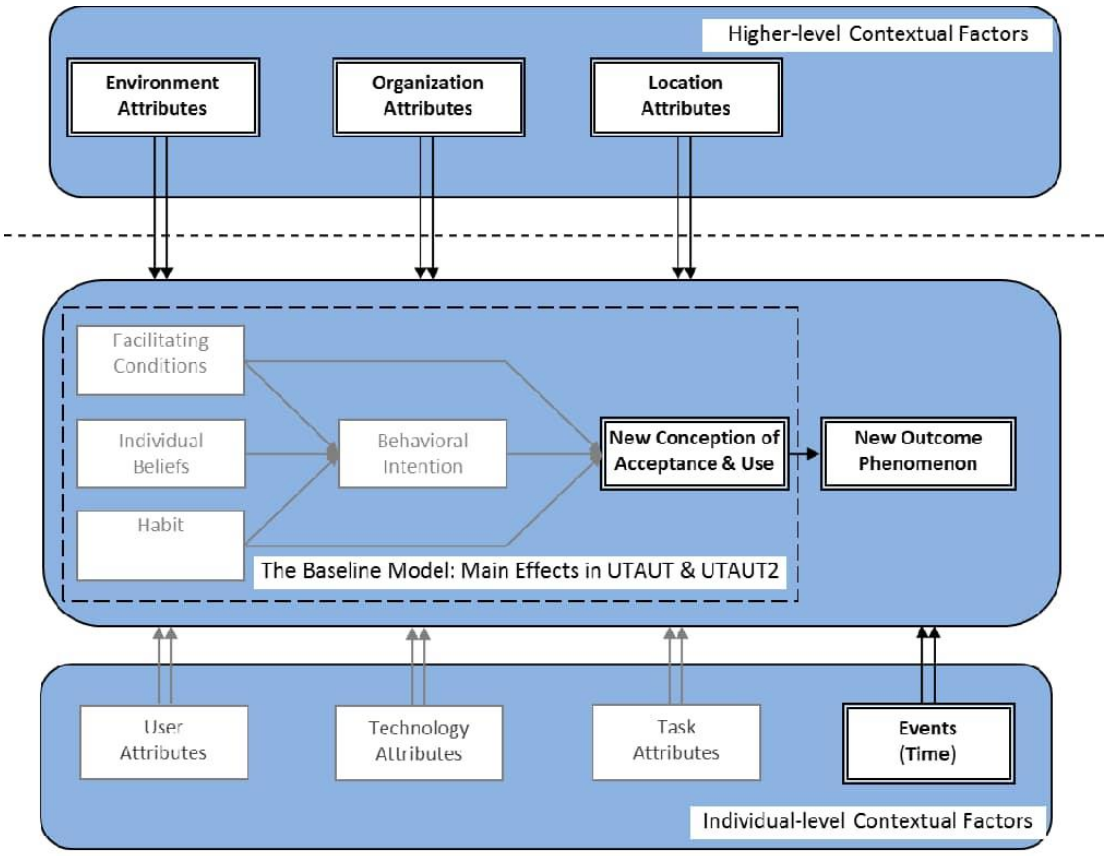
1.1.2 النظرية الموحدة لقبول واستخدام التكنولوجيا (UTAUT)

في محاولة لتوحيد النماذج المتعددة لقبول التكنولوجيا وتجاوز حدود النماذج الفردية، طور فينكاتيش وزملاؤه النظرية الموحدة لقبول واستخدام التكنولوجيا (Unified Theory of Acceptance and Use of Technology – UTAUT) عام 2003 . تمثل UTAUT تكاملاً شاملاً لثمانية نماذج رئيسية لقبول التكنولوجيا، بما في ذلك نموذج قبول التكنولوجيا (TAM) ، ونظرية السلوك المخطط (TPB) ، ونظرية انتشار الابتكار (IDT) (Xue et al., 2024).

تقوم UTAUT على أربعة محددات رئيسية للنية السلوكية واستخدام التكنولوجيا:

1. توقعات الأداء (Performance Expectancy): الدرجة التي يعتقد بها الفرد أن استخدام النظام سيساعده على تحقيق مكاسب في أدائه الوظيفي.
2. توقعات الجهد (Effort Expectancy): سهولة استخدام النظام المدركة.
3. التأثير الاجتماعي (Social Influence): مدى إدراك الفرد لأهمية اعتقاد الآخرين بضرورة استخدامه للنظام الجديد.

الظروف الميسرة (Facilitating Conditions): درجة اعتقاد الفرد بتوافر البنية التحتية التنظيمية والتقنية اللازمة لدعم استخدام النظام.(Venkatesh et al., 2003; Ayaz & Yanartaş, 2020)



Notes:
1. Single arrows represent the main effects.
2. Double arrows represent the main effects or moderation effects of contextual factors.
3. Double-line boxes represent the important areas for future UTAUT extensions.

الشكل 2 النظرية الموحدة لقبول واستخدام التكنولوجيا – (UTAUT)

أظهرت الاختبارات التطبيقية أن نموذج UTAUT يفسر حوالي 70% من التباين في النية السلوكية لاستخدام التكنولوجيا، وهو ما يمثل قوة تنبؤية أعلى مقارنةً بالنماذج الأخرى (Venkatesh et al., 2016; Xue et al., 2024). كما أن النموذج يأخذ في الاعتبار أربعة متغيرات معدّلة هي: العمر، والجنس، والخبرة، وطوعية الاستخدام، والتي تؤثر على قوة العلاقة بين المحددات الرئيسية والنية السلوكية (Venkatesh et al., 2003).

النموذج	نسبة التباين المفسّر	عدد المحددات الرئيسية	المتغيرات المعدّلة	مجال التطبيق الأساسي
TAM	40–50%	2	لا يوجد	بيئة العمل
TAM2	52–60%	5	الخبرة، الطوعية	بيئة العمل
UTAUT	70%	4	العمر، الجنس، الخبرة، الطوعية	بيئة العمل
UTAUT2	74%	7	العمر، الجنس، الخبرة	السياق الاستهلاكي

جدول5 مقارنة بين قوة النماذج التنبؤية لقبول التكنولوجيا

في عام 2012، قام فينكاتيش وزملاؤه بتطوير نسخة موسعة من النموذج تُعرف بـ UTAUT2، والتي أُعدت خصيصاً لفهم تبني التكنولوجيا في السياق الاستهلاكي. أضافت UTAUT2 ثلاثة محددات جديدة هي:

- الحافز الترفيهي (Hedonic Motivation): المتعة أو التسلية المستمدة من استخدام التكنولوجيا.
- قيمة السعر (Price Value): المفاضلة بين الفوائد المدركة والتكلفة المالية.
- العادة (Habit): المدى الذي يميل فيه الأفراد لأداء السلوكيات تلقائياً بسبب التعلم.

مما رفع القوة التفسيرية للنموذج إلى 74% من التباين في النية السلوكية (Venkatesh et al., 2012). أثبتت الدراسات التطبيقية في قطاع الخدمات المالية أن توقعات الأداء تمثل أقوى محدد للنية السلوكية لاستخدام تطبيقات التكنولوجيا المالية، تليها توقعات الجهد والتأثير الاجتماعي (Xue et al., 2024; Williams et al., 2015).

1.2 دور الثقة في نماذج تبني التكنولوجيا

رغم القوة التفسيرية العالية لنماذج TAM وUTAUT، أشارت الأبحاث إلى أهمية إدماج متغير الثقة (Trust) كعامل محوري في سياق الخدمات المالية الرقمية (Jafri et al., 2023). تُعرّف الثقة في البيئة الرقمية بأنها اعتقاد المستخدم بأن مزود الخدمة التقني يتمتع بالنزاهة والمصداقية والقدرة على حماية المعلومات الحساسة (Gefen et al., 2003). في القطاع المالي، حيث تنطوي المعاملات على مخاطر مالية مباشرة وتتطلب مشاركة بيانات شخصية ومالية حساسة، تصبح الثقة عاملاً حاسماً في قرار التبني (Jafri et al., 2023).

أظهرت دراسة حديثة دمجت UTAUT2 مع نموذج الثقة النظري أن الثقة تلعب دوراً محورياً في التأثير على كل من النية لاستخدام خدمات التكنولوجيا المالية والاستخدام الفعلي لها. وجدت الدراسة أن الثقة لا تؤثر فقط بشكل مباشر على النية السلوكية، بل تعمل أيضاً كمتغير وسيط بين المحددات الأساسية لـ UTAUT والنية لاستخدام التطبيقات المالية (Al-Sharafi et al., 2023). كما أن إدراك المخاطر المرتبطة بالأمن السيبراني والخصوصية يؤثر سلباً على الثقة، مما يؤدي بدوره إلى انخفاض معدلات التبني(Aljaradat et al., 2024).

المحدد	التأثير المباشر	دور الثقة كمتغير وسيط	الأهمية النسبية
توقعات الأداء	قوي(+)	الثقة تعزز التأثير	عالية جداً
توقعات الجهد	متوسط(+)	الثقة تعزز التأثير	عالية
التأثير الاجتماعي	متوسط(+)	الثقة تعزز التأثير	متوسطة
الظروف الميسرة	ضعيف(+)	الثقة لا تؤثر كثيراً	منخفضة
الثقة	قوي جداً(+)	–	عالية جداً

جدول6 تأثير الثقة على محددات UTAUT في سياق التطبيقات المالية

المصدر: مستخلص من (Al-Sharafi et al., 2023; Jafri et al., 2023)

في سياق تطبيقات الدفع الإلكتروني، تتشكل الثقة من ثلاثة أبعاد رئيسية:

1. الثقة في التكنولوجيا نفسها(Technology Trust): الاعتقاد بأن التطبيق مصمم بطريقة آمنة وموثوقة.

2. الثقة في المؤسسة المقدمة للخدمة(Institutional Trust): الثقة في سمعة ومصداقية مزود الخدمة.

3. الثقة في البيئة التنظيمية والقانونية(Regulatory Trust): الثقة في قدرة الجهات التنظيمية على حماية حقوق المستخدمين.

تُظهر الدراسات أن الإجراءات الأمنية الفعالة، مثل التشفير والمصادقة متعددة العوامل، تعزز الثقة في التكنولوجيا، بينما تساهم السمعة المؤسسية والشفافية في تعزيز الثقة في مزود الخدمة (Jafri et al., 2023).

2. نظريات الثقة في البيئة الرقمية

2.1 المفاهيم الأساسية للثقة في المعاملات الإلكترونية

تُعد الثقة عنصراً محورياً في نجاح الخدمات المالية الرقمية، إذ تمثل الأساس الذي يُبنى عليه استعداد المستخدمين للمشاركة في المعاملات الإلكترونية ومشاركة معلوماتهم الحساسة (McKnight et al., 2002). في البيئة الرقمية، حيث تغيب التفاعلات الوجاهية المباشرة وتزداد المخاطر المدركة، تصبح الثقة أكثر أهمية من السياقات التقليدية (Kim et al., 2008). تُعرّف الثقة في الخدمات المالية الرقمية بأنها الاستعداد النفسي للفرد لقبول الضعف أمام تصرفات مزود الخدمة، بناءً على توقعات إيجابية بشأن نواياه وقدراته (Mayer et al., 1995).

تتكون الثقة من ثلاثة مكونات رئيسية وفقاً لنموذج (Mayer et al., 1995):

1. القدرة (Ability): امتلاك مزود الخدمة للمهارات والكفاءات التقنية اللازمة لتقديم خدمة آمنة وموثوقة.
2. النزاهة (Integrity): التزام المؤسسة بمبادئ أخلاقية وقيم يقبلها المستخدم.

3. الإحسان (Benevolence): الاعتقاد بأن مزود الخدمة يهتم بمصلحة المستخدم ويسعى لتحقيق منفعته بغض النظر عن الدافع الربحي.

المكون	التعريف	مؤشرات القياس	أمثلة تطبيقية
القدرة	الكفاءة التقنية والمهنية	-جودة الخدمة -موثوقية النظام -سرعة المعاملات	-استخدام تشفير متقدم -ضمان توفر الخدمة 7/24 -معالجة سريعة للمعاملات
النزاهة	الالتزام الأخلاقي والشفافية	-الصدق في التواصل -الوفاء بالوعود -الامتثال للوائح	-سياسات خصوصية واضحة -إفصاح عن الرسوم -الحصول على شهادات أمنية
الإحسان	الاهتمام بمصلحة المستخدم	-الاستجابة للشكاوى -تقديم دعم فني -حماية مصالح العملاء	-خدمة عملاء ممتازة -تأمين على الودائع -إشعارات استباقية بالمخاطر

جدول7 مكونات الثقة وتطبيقاتها في الخدمات المالية الرقمية

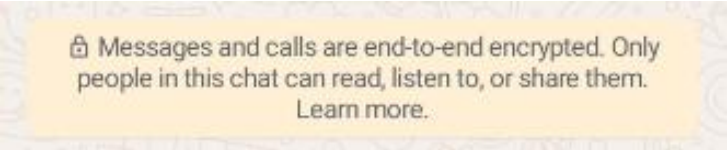
2.2 أبعاد الثقة في تطبيقات الدفع الإلكتروني

تتخذ الثقة في تطبيقات الدفع الإلكتروني أبعاداً متعددة تشمل الثقة في التكنولوجيا، والثقة في المؤسسة، والثقة في الإطار التنظيمي (Jafri et al., 2023) .

1. الثقة في التكنولوجيا

تشير الثقة في التكنولوجيا إلى اعتقاد المستخدم بأن التطبيق مصمم بطريقة آمنة وموثوقة، وأنه يتضمن آليات حماية فعالة ضد الاختراقات والاحتيال(McKnight et al., 2002). تتحقق هذه الثقة من خلال تنفيذ تقنيات أمنية متقدمة مثل:

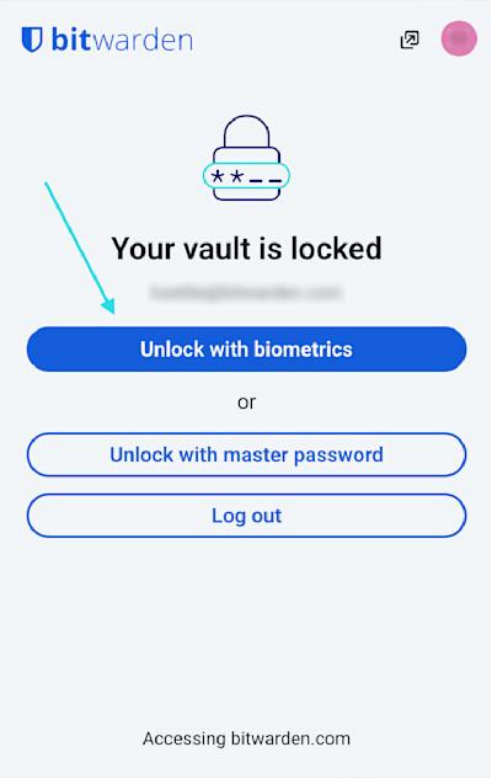
- التشفير من طرف إلى طرف (End-to-End Encryption): يضمن أن البيانات تُشفّر على جهاز المستخدم ولا يمكن فك تشفيرها إلا من قبل المستلم المقصود. كالتشفير المستخدم في بعض تطبيقات المحادثة الفورية كال WhatsApp.



الشكل 3 رسالة مشفرة من طرف إلى طرف

- المصادقة متعددة العوامل (Multi-Factor Authentication): تضيف طبقات أمان إضافية من خلال طلب أكثر من شكل واحد من أشكال التحقق. كإدخال كلمة السر ورمز التحقق المرسل كرسالة SMS.

المصادقة البيومترية (Biometric Authentication): استخدام بصمة الإصبع أو التعرف على الوجه لتوفير مستوى عالٍ من الأمان.(Akitra, 2025; Fintech Strategy, 2024)



الشكل 4 يظهر تطبيقاً يطلب مصادقة بيومترية

2. الثقة في المؤسسة

تتعلق الثقة في المؤسسة بسمعة مزود الخدمة وتاريخه في السوق، إذ يميل المستخدمون إلى الثقة بشكل أكبر في التطبيقات المرتبطة بمؤسسات مالية راسخة أو بشركات تتمتع بسمعة طيبة (McKnight et al., 2002). أظهرت دراسة أُجريت في دول جنوب شرق آسيا أن الثقة في البنوك التقليدية لا تزال أعلى من الثقة في مزودي الخدمات المالية الرقمية غير البنكية، رغم أن الفارق ليس كبيراً (Tech For Good Institute, 2025).

يشير ذلك إلى أهمية الشراكات بين شركات التكنولوجيا المالية والمؤسسات المالية التقليدية في تعزيز الثقة لدى المستخدمين.

3. الثقة في الإطار التنظيمي

تعكس الثقة في الإطار التنظيمي ثقة المستخدمين في قدرة الجهات التنظيمية والقانونية على حماية حقوقهم وفرض الامتثال للمعايير الأمنية ومعايير حماية البيانات (Jafri et al., 2023). في البلدان التي تتمتع بأطر تنظيمية قوية وواضحة للخدمات المالية الرقمية، يكون المستخدمون أكثر استعداداً لتبني هذه التقنيات (World Bank, 2025). تلعب اللوائح مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا دوراً مهماً في تعزيز ثقة المستخدمين من خلال ضمان حقوقهم في الخصوصية والأمان (Doerr et al., 2023).

البُعد	العوامل الإيجابية	العوامل السلبية	الأهمية النسبية
الثقة في التكنولوجيا	-تقنيات تشفير متقدمة -مصادقة بيومترية -تحديثات أمنية منتظمة	-ثغرات أمنية -بطء الأداء -أعطال متكررة	35%

البُعد	العوامل الإيجابية	العوامل السلبية	الأهمية النسبية
الثقة في المؤسسة	-سمعة قوية -شراكات مع بنوك -شفافية في التعاملات	-حوادث اختراق سابقة -شكاوى العملاء -غموض في السياسات	40%
الثقة في الإطار التنظيمي	-قوانين حماية واضحة -جهات رقابية فعالة -عقوبات رادعة	-غياب التنظيم -ضعف التنفيذ -غموض قانوني	25%

جدول8 العوامل المؤثرة على أبعاد الثقة في تطبيقات الدفع الإلكتروني

المصدر: مستخلص من (Jafri et al., 2023; Tech For Good Institute, 2025)

3. الأمن السيبراني في الخدمات المالية الرقمية

3.1 الإطار المفاهيمي للأمن السيبراني

3.1.1 مفهوم الأمن السيبراني وأهميته

يُعرّف الأمن السيبراني بأنه مجموعة الإجراءات والتقنيات والممارسات المصممة لحماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية والوصول غير المصرح به والأضرار (National Institute of Standards and Technology, 2018). في سياق الخدمات المالية الرقمية، يكتسب الأمن السيبراني أهمية بالغة نظراً لحساسية البيانات المالية والشخصية التي يتم تداولها، والعواقب الوخيمة المحتملة للاختراقات الأمنية (Frost, 2025).

مع التوسع السريع في استخدام المدفوعات الرقمية على مستوى العالم، تزايدت التهديدات السيبرانية بشكل متناسب، إذ أصبحت الأنظمة المالية الرقمية أهدافاً جذابة للمجرمين الإلكترونيين (Akitra, 2025). تشير التقارير إلى أن القطاع المالي تجاوز قطاع الرعاية الصحية ليصبح القطاع الأكثر تعرضاً لخروقات البيانات في عام 2023، حيث بلغ متوسط تكلفة الاختراق الأمني في المؤسسات المالية 6.08مليون دولار أمريكي، وهو أعلى بكثير من المتوسط العالمي عبر القطاعات (Thales Group, 2025). هذا يؤكد الحاجة الملحة إلى تبني استراتيجيات أمن سيبراني شاملة ومتقدمة.

يهدف الأمن السيبراني في الخدمات المالية إلى تحقيق ثلاثة أهداف رئيسية معروفة باسم ثالوث:CIA

1. السرية (Confidentiality): حماية المعلومات الحساسة من الوصول غير المصرح به.

2. النزاهة (Integrity): الحفاظ على دقة البيانات وكمالها ومنع تعديلها بشكل غير مشروع.

3. التوافرية (Availability): ضمان إمكانية الوصول إلى الأنظمة والبيانات من قبل المستخدمين المصرح لهم في الوقت المناسب.

(National Institute of Standards and Technology, 2018; Fintech Strategy, 2024)

الشكل 5 أهداف الأمن السيبراني CIA

القطاع	متوسط التكلفة (مليون دولار)	نسبة الزيادة عن 2022	متوسط الوقت لاكتشاف الاختراق (يوم)
القطاع المالي	6.08	+8.2%	233
الرعاية الصحية	5.93	+6.5%	207
الأدوية	5.01	+4.8%	198

القطاع	متوسط التكلفة (مليون دولار)	نسبة الزيادة عن 2022	متوسط الوقت لاكتشاف الاختراق (يوم)
التكنولوجيا	4.97	+7.1%	214
الطاقة	4.78	+5.3%	221
المتوسط العالمي	4.45	+6.7%	227

جدول9 تكاليف اختراقات البيانات حسب القطاع (2023)

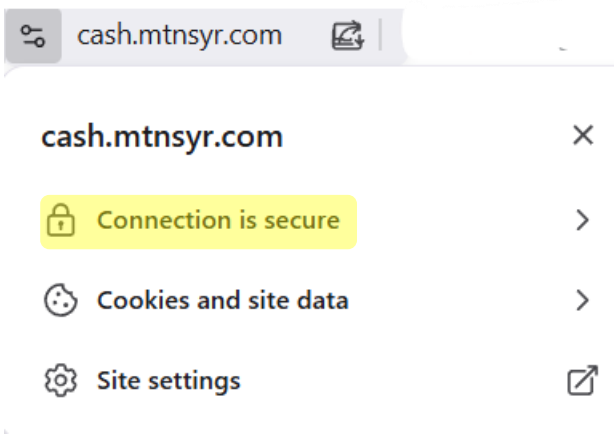
المصدر (Thales Group, 2025)

3.1.2 مكونات الأمن السيبراني في تطبيقات الدفع الإلكتروني

تتكون البنية الأمنية لتطبيقات الدفع الإلكتروني من عدة طبقات متكاملة تعمل معاً لضمان حماية شاملة (Akitra, 2025). تشمل هذه المكونات:

1. التشفير (Encryption)

يُعد التشفير حجر الزاوية في أمن البيانات المالية، إذ يحول البيانات الحساسة إلى صيغة غير قابلة للقراءة لا يمكن فك شفرتها إلا باستخدام مفتاح التشفير الصحيح .(Fintech Strategy, 2024) تستخدم تطبيقات الدفع الحديثة معايير تشفير متقدمة مثل AES-256 لحماية البيانات أثناء النقل والتخزين، مما يضمن عدم إمكانية اعتراضها وقراءتها حتى في حالة الاختراق (Metomic, 2025).



الشكل 6 يظهر إستخدام التشفير بموقع MTN Cash

2. المصادقة متعددة العوامل (Multi-Factor Authentication – MFA)

تضيف المصادقة متعددة العوامل طبقة أمان إضافية من خلال مطالبة المستخدمين بتقديم أكثر من شكل واحد من أشكال التحقق من الهوية قبل منح الوصول إلى الحساب (Fintech Strategy, 2024). قد تتضمن هذه العوامل:

- شيء يعرفه المستخدم :كلمة المرور أو رقم التعريف الشخصي(PIN) .
- شيء يملكه المستخدم :رمز لمرة واحدة عبر الرسائل النصية أو تطبيق مصادق.

- شيء يمثله المستخدم :البصمة البيومترية (بصمة الإصبع، التعرف على الوجه).

(Akitra, 2025)

3. المصادقة البيومترية (Biometric Authentication)

تستخدم العديد من التطبيقات المالية الحديثة تقنيات المصادقة البيومترية مثل بصمة الإصبع والتعرف على الوجه لتوفير مستوى عالٍ من الأمان مع الحفاظ على تجربة مستخدم سلسة (Fintech Strategy, 2024). تتميز هذه التقنية بصعوبة تزويرها مقارنةً بكلمات المرور التقليدية، مما يعزز الأمان بشكل كبير.

الشكل 7 يظهر المصادقة المتعددة بطلب PIN أو المصادقة البيومترية

4. الترميز (Tokenization)

تتضمن عملية الترميز استبدال البيانات المالية الحساسة، مثل أرقام البطاقات، برموز فريدة لا قيمة لها خارج سياق المعاملة المحددة (Fintech Strategy, 2024). حتى في حالة اعتراض هذه الرموز، لا يمكن استخدامها في معاملات أخرى، مما يقلل بشكل كبير من مخاطر الاحتيال.

التقنية	مستوى الأمان	التأثير على تجربة المستخدم	التكلفة النسبية	معدل الاعتماد
كلمة المرور فقط	منخفض	سلس جداً	منخفضة جداً	100%
كلمة المرور + OTP	متوسط	متوسط (تأخير بسيط)	منخفضة	75%
المصادقة البيومترية	عالٍ	سلس جداً	متوسطة	60%
MFA الكامل	عالٍ جداً	أقل سلاسة	متوسطة–عالية	40%

التقنية	مستوى الأمان	التأثير على تجربة المستخدم	التكلفة النسبية	معدل الاعتماد
التشفير من طرف لطرف	عالٍ جداً	شفاف للمستخدم	عالية	85%
الترميز	عالٍ جداً	شفاف للمستخدم	عالية	70%

جدول10 مقارنة بين تقنيات الأمان المختلفة في تطبيقات الدفع الإلكتروني

3.1.3 التهديدات السيبرانية الشائعة

تواجه تطبيقات الدفع الإلكتروني مجموعة متنوعة من التهديدات السيبرانية التي تتطور باستمرار مع تقدم التكنولوجيا (Akitra, 2025). من أبرز هذه التهديدات:

أ. هجمات التصيد الاحتيالي (Phishing Attacks)

تُعد هجمات التصيد من أكثر أساليب الاحتيال شيوعاً، حيث يستخدم المهاجمون رسائل بريد إلكتروني أو رسائل نصية مزيفة لخداع الضحايا وحملهم على الكشف عن معلوماتهم الحساسة مثل بيانات تسجيل الدخول والتفاصيل المالية (Fintech Strategy, 2024). تصبح هذه الهجمات أكثر تعقيداً مع استخدام تقنيات الهندسة الاجتماعية المتطورة (Akitra, 2025).

ب. اختراقات البيانات (Data Breaches)

تحدث اختراقات البيانات عندما يحصل أطراف غير مصرح لهم على وصول إلى قواعد بيانات المؤسسات المالية، مما يؤدي إلى تسريب كميات ضخمة من المعلومات الحساسة بما في ذلك البيانات الشخصية والمالية للمستخدمين (Fintech Strategy, 2024). تشير الإحصاءات إلى أن القطاع المالي أصبح الأكثر استهدافاً في السنوات الأخيرة (Thales Group, 2025).

ج. البرمجيات الخبيثة وبرامج الفدية (Malware and Ransomware)

تستخدم برامج الفدية أساليب خبيثة لاختراق الأنظمة الحاسوبية وسرقة البيانات أو مراقبة الأنشطة أو قفل الحسابات، ثم يطالب المهاجمون بدفع فدية لاستعادة الوصول أو منع نشر البيانات (Fintech Strategy, 2024). يمكن أن تسبب هذه الهجمات اضطرابات كبيرة في الخدمات وخسائر مالية فادحة.

د. هجمات حشو بيانات الاعتماد (Credential Stuffing)

تستغل هذه الهجمات ميل المستخدمين لإعادة استخدام نفس أسماء المستخدمين وكلمات المرور عبر منصات متعددة، حيث يستخدم المهاجمون بيانات اعتماد مسروقة من اختراقات سابقة للحصول على وصول غير مصرح به إلى حسابات أخرى (Fintech Strategy, 2024).

نوع التهديد	احتمالية الحدوث	التأثير المحتمل	أبرز الأمثلة	الإجراء الوقائي الرئيسي
التصيد الاحتيالي	عالية جداً	متوسط–عالي	رسائل انتحال هوية البنوك	التوعية والتدريب
اختراق البيانات	متوسطة	عالٍ جداً	تسريب معلومات العملاء	التشفير والتحكم بالوصول
برامج الفدية	متوسطة	عالٍ جداً	تجميد الأنظمة المصرفية	النسخ الاحتياطي والتحديثات
حشو البيانات	عالية	متوسط	اختراق حسابات بكلمات مرور مكررة	MFAوسياسات كلمات مرور قوية
هجمات DDoS	متوسطة–عالية	متوسط	تعطيل الخدمات المصرفية	بنية تحتية مرنة

جدول 11 أنواع التهديدات السيبرانية وتأثيرها على القطاع المالي

3.2 إدارة مخاطر الأمن السيبراني

3.2.1 مفهوم إدارة المخاطر السيبرانية

تُعرّف إدارة مخاطر الأمن السيبراني بأنها عملية منهجية لتحديد وتقييم ومعالجة المخاطر المرتبطة بالتهديدات السيبرانية لحماية أصول المعلومات والبنية التحتية التقنية (Xygeni, 2025). تهدف هذه العملية إلى تقليل احتمالية حدوث الحوادث الأمنية وتخفيف تأثيرها المحتمل على المؤسسة وعملائها (Bakkah, 2025). في سياق الخدمات المالية الرقمية، تصبح إدارة المخاطر السيبرانية أولوية استراتيجية نظراً للطبيعة الحساسة للبيانات المالية والعواقب الوخيمة للاختراقات الأمنية على سمعة المؤسسة وثقة العملاء (Visure Solutions, 2025).

تتكون عملية إدارة المخاطر السيبرانية من عدة مراحل رئيسية:

1. التحديد: جرد شامل لأصول المعلومات والأنظمة الحرجة، وتحديد التهديدات المحتملة
2. التقييم: تحليل نقاط الضعف في الأنظمة واحتمالية استغلالها
3. التحليل: تحليل المخاطر من حيث احتمالية الحدوث والتأثير المحتمل
4. المعالجة: اتخاذ قرارات استراتيجية (التخفيف، التجنب، النقل، القبول)
5. المراقبة المستمرة: متابعة فعالية الضوابط والتهديدات الجديدة

(Xygeni, 2025; Bakkah, 2025)

3.2.2 أطر عمل إدارة المخاطر السيبرانية

تعتمد المؤسسات المالية على أطر عمل معترف بها دولياً لتوجيه جهودها في إدارة المخاطر السيبرانية. من أبرز هذه الأطر:

أ. إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST Cybersecurity Framework).

طوّر المعهد الوطني للمعايير والتكنولوجيا الأمريكي هذا الإطار الطوعي لمساعدة المؤسسات على فهم وتقييم وترتيب أولويات وتوصيل جهودها في مجال الأمن السيبراني لإدارة المخاطر الإلكترونية والحد منها (NIST, 2018). يتكون الإطار من ست وظائف رئيسية:

1. الحوكمة (Govern): الأساس الاستراتيجي لإدارة المخاطر السيبرانية.
2. التحديد (Identify): فهم السياق التنظيمي والموارد والمخاطر.
3. الحماية (Protect): تطوير وتنفيذ الضوابط الأمنية.
4. الكشف (Detect): تحديد الأحداث الأمنية في الوقت المناسب.
5. الاستجابة (Respond): التعامل مع الحوادث المكتشفة.
6. التعافي (Recover): استعادة الخدمات والعمليات بسرعة.

(NIST, 2018; Hyperproof, 2025)

ب. معيار ISO/IEC 27001

يُعد هذا المعيار الدولي أحد أبرز معايير إدارة أمن المعلومات، ويوفر إطاراً منهجياً لإنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات (ISMS) (ISMS Online, 2025). يركز المعيار على تحديد وتقييم ومعالجة مخاطر أمن المعلومات من خلال نهج دورة حياة Plan–Do–Check–Act.

وجه المقارنة	NIST Cybersecurity Framework	ISO/IEC 27001
الطبيعة	إطار طوعي توجيهي	معيار قابل للشهادة
النطاق	الأمن السيبراني بشكل أساسي	أمن المعلومات بشكل شامل
التطبيق	مرن وقابل للتخصيص	منظم ومحدد
الشهادة	لا توجد شهادة رسمية	شهادة معترف بها دولياً
التركيز	إدارة المخاطر السيبرانية	نظام إدارة أمن المعلومات
الملاءمة	جميع القطاعات	جميع القطاعات
التكلفة	مجاني	يتطلب استثماراً للحصول على الشهادة

وجه المقارنة	NIST Cybersecurity Framework	ISO/IEC 27001
التحديثات	دورية (آخر تحديث 2024)	دورية (آخر تحديث 2022)

جدول 12 مقارنة بين إطار NIST ومعيار ISO 27001

المصدر: (ISMS Online, 2025; AuditBoard, 2025; OneTrust, 2025)

رغم الاختلافات، يمكن للمؤسسات دمج كلا الإطارين للاستفادة من نقاط قوة كل منهما، حيث يوفر NIST مرونة أكبر ومستويات نضج محددة، بينما يقدم ISO 27001 نهجاً أكثر تنظيماً وإمكانية الحصول على شهادة معترف بها دولياً (ISMS Online, 2025; OneTrust, 2025).

4. التسويق الرقمي للخدمات المالية

4.1 أسس التسويق الرقمي في القطاع المالي

4.1.1 مفهوم التسويق الرقمي وأهميته

يُعرّف التسويق الرقمي في الصناعة المالية بأنه الاستراتيجيات والتكتيكات التي تستخدمها المؤسسات المالية لترويج عروضها وإشراك العملاء وتوسيع قاعدة عملائها من خلال القنوات الرقمية (Landingi, 2025). ويُنظر إلى التسويق الرقمي على أنه امتداد وتطوير لمفهوم التسويق التقليدي، لا مجرد بديل عنه، حيث يبقى جوهر العملية التسويقية قائماً على فهم حاجات الزبائن وإشباعها، لكن بأدوات جديدة تعتمد الموقع الإلكتروني، والبريد الإلكتروني، ومحركات البحث، ومنصات التواصل الاجتماعي، وتطبيقات الهواتف الذكية وغيرها من الوسائط الرقمية التي تتيح للشركات الوصول إلى أسواق أوسع، والتواصل الآني، وجمع البيانات وتحليلها بصورة مستمرة لدعم اتخاذ القرار التسويقي (النجار, 2021). تستفيد الخدمات المالية، بما في ذلك البنوك وشركات التأمين وشركات الاستثمار وشركات التكنولوجيا المالية، من منصات إلكترونية متنوعة مثل وسائل التواصل الاجتماعي والبريد الإلكتروني والتسويق بالمحتوى وغيرها للتواصل مع العملاء المحتملين وبناء علاقات قوية ودائمة (Landingi, 2025).

يساعد التسويق الرقمي الفعال المؤسسات المالية ليس فقط على الوصول إلى جمهورها المستهدف، بل أيضاً على بناء الثقة والمصداقية، وهو أمر بالغ الأهمية في مجال يُعطي فيه المستهلكون الأولوية للأمان والموثوقية (Landingi, 2025; Fully Vested, 2025). على عكس التسويق التقليدي، يُمكّن التسويق الرقمي من تقديم محتوى ذي صلة في الوقت المناسب يُعلِم ويبني الثقة مع تحسين تجارب العملاء (Landingi, 2025).

وجه المقارنة	التسويق التقليدي	التسويق الرقمي
القنوات	إعلانات تلفزيونية، صحف، لوحات إعلانية	وسائل التواصل الاجتماعي، محركات البحث، البريد الإلكتروني
التكلفة	عالية جداً	متوسطة–منخفضة
الاستهداف	جماهير عامة واسعة	استهداف دقيق حسب الديموغرافيا
القياس	صعب ومحدود	سهل ودقيق (Analytics)
التفاعل	أحادي الاتجاه	ثنائي الاتجاه
المرونة	محدودة	عالية جداً
الوصول الجغرافي	محلي/إقليمي	عالمي
ROI	صعب القياس	قابل للقياس الدقيق

جدول13 الفروقات بين التسويق التقليدي والتسويق الرقمي في القطاع المالي

4.1.2 استراتيجيات التسويق الرقمي الأساسية

تتضمن الاستراتيجيات الفعالة للتسويق الرقمي في القطاع المالي عدة مكونات رئيسية :

1. فهم الجمهور المستهدف وخدمته

يبدأ التسويق الرقمي الفعال للخدمات المالية بفهم شامل للجمهور المستهدف .من خلال تحديد العميل المثالي والقطاعات المتخصصة، يمكن للمؤسسات تخصيص رسائلها لمعالجة التحديات المالية المحددة، وتمييز علامتها التجارية عن المنافسين، وزيادة حصتها السوقية.(Three29, 2025)

2. المحتوى التعليمي والقيادة الفكرية

يُعد إنشاء محتوى تعليمي عالي الجودة أمراً أساسياً لبناء الثقة والمصداقية (Fully Vested, 2025; Neil Patel, 2025). يساعد المحتوى التثقيفي العملاء على فهم المنتجات المالية المعقدة واتخاذ قرارات مستنيرة، مما يعزز مكانة المؤسسة كسلطة موثوقة في المجال.

3. تحسين محركات البحث المحلية (Local SEO)

بالنسبة للمؤسسات المالية التي تخدم مناطق جغرافية محددة، يُعد تحسين محركات البحث المحلية أمراً بالغ الأهمية لتحسين الظهور في عمليات البحث الإقليمية (Neil Patel, 2025). يتضمن ذلك تحسين صفحات الأعمال على Google وBing، واستخدام الكلمات المفتاحية المحلية، وإنشاء محتوى ذي صلة بالمنطقة المستهدفة.

4.التخصيص والمحتوى المُخصص

يتيح استخدام البيانات لإنشاء حملات مستهدفة تقديم محتوى وعروض مُخصصة بناءً على تفضيلات العملاء وسلوكياتهم، مما يزيد من التفاعل والرضا (Fully Vested, 2025; Landingi, 2025). وفقاً لـHubSpot ، تشهد الشركات التي تتفاعل مع العملاء عبر وسائل التواصل الاجتماعي زيادة في الإيرادات تتراوح بين 20–40 % (Fully Vested, 2025).

5. التسويق متعدد القنوات (Omnichannel Marketing)

تتغير نقاط الاتصال مع العملاء من عدد قليل من نقاط الاتصال واسعة النطاق (مثل زيارات البنوك) على مدار العام إلى سلسلة من نقاط الاتصال الأصغر حجماً، حيث يتفاعل المستهلكون مع العلامة التجارية بشكل منتظم إلى حد ما. تساعد الاستراتيجية متعددة القنوات في بناء الثقة والولاء من خلال التواصل المستمر عبر منصات متعددة بما في ذلك وسائل التواصل الاجتماعي والتطبيقات وحتى الرسائل النصية القصيرة (EVERFI, 2025).

القناة	معدل التفاعل	معدل التحويل	التكلفة لكل عميل	الملاءمة للخدمات المالية
محركات البحث (SEO/SEM)	متوسط	عالٍ	متوسطة	عالية جداً

القناة	معدل التفاعل	معدل التحويل	التكلفة لكل عميل	الملاءمة للخدمات المالية
وسائل التواصل الاجتماعي	عالٍ جداً	متوسط	منخفضة	عالية
البريد الإلكتروني	متوسط–عالي	عالٍ جداً	منخفضة جداً	عالية جداً
التسويق بالمحتوى	عالٍ	متوسط–عالي	متوسطة	عالية جداً
الإعلانات المدفوعة	متوسط	متوسط–عالي	عالية	متوسطة–عالية
التسويق بالفيديو	عالٍ جداً	عالٍ	متوسطة–عالية	عالية

جدول 14 فعالية قنوات التسويق الرقمي في القطاع المالي

4.2 التسويق الأمني والحملات التوعوية

4.2.1 أهمية التسويق الأمني

يُعد التسويق الأمني جانباً حاسماً من جوانب استراتيجية التسويق الرقمي للخدمات المالية، إذ يهدف إلى تعزيز ثقة العملاء من خلال إبراز التزام المؤسسة بحماية بياناتهم وأموالهم (Thales Group, 2025). في عصر تتزايد فيه التهديدات السيبرانية والمخاوف بشأن الخصوصية، أصبح إظهار الإجراءات الأمنية القوية عاملاً تنافسياً أساسياً للمؤسسات المالية (The Financial Brand, 2024).

تشير الأبحاث إلى أن ثقة المستهلكين في المؤسسة تؤثر بشكل كبير على مستوى ارتياحهم تجاه استخدام الذكاء الاصطناعي ومشاركة البيانات، مع زيادة في مستوى الراحة تبلغ 11نقطة مئوية بين أولئك الذين يثقون بالمؤسسة. بالنسبة للبنوك، يشير ذلك إلى أن بناء الثقة من خلال التواصل الشفاف حول استخدام الذكاء الاصطناعي والبيانات يجب أن يسبق إطلاق المبادرات التكنولوجية الجديدة (The Financial Brand, 2024).

4.2.2 عناصر الحملات التسويقية الأمنية الفعالة

تتضمن الحملات التسويقية الأمنية الناجحة عدة عناصر رئيسية:

1. الشفافية في استخدام البيانات

يُظهر العملاء احتمالية أكبر بمقدار 1.7 مرة لمشاركة بياناتهم عندما يفهمون بالضبط كيف سيتم استخدامها. توفير خيارات واضحة للاشتراك/عدم الاشتراك يزيد من الراحة في مشاركة البيانات بنسبة 42%، بينما التحديثات المنتظمة حول استخدام البيانات تزيد الثقة بنسبة 38% (The Financial Brand, 2024).

2. تبادل القيمة (Value Exchange)

يستعد 72% من العملاء لمشاركة بياناتهم عندما يحصلون على قيمة واضحة في المقابل، تُعد الرؤى المالية والتوصيات المُخصصة للمنتجات من الفوائد الأكثر قيمة، بينما يُبرر كشف الاحتيال في الوقت الفعلي وميزات الأمان جمع البيانات في أذهان العملاء (The Financial Brand, 2024).

3. التواصل المستمر والتعليم

يتطلب بناء الثقة تواصلاً مستمراً حول الإجراءات الأمنية المطبقة وكيفية حماية بيانات العملاء (Thales Group, 2025). يجب أن تتضمن الحملات التسويقية محتوى تعليمياً يساعد العملاء على فهم المخاطر الأمنية وكيفية حماية أنفسهم، مما يعزز ثقتهم في المؤسسة (Frost, 2025).

4. إظهار الامتثال والشهادات

يُعد عرض الامتثال للمعايير الأمنية الدولية والحصول على شهادات معترف بها مثل ISO 27001 و PCI DSS وسيلة فعالة لبناء الثقة (Thales Group, 2025). يُظهر ذلك للعملاء أن المؤسسة تأخذ الأمان على محمل الجد وتلتزم بأفضل الممارسات الصناعية.

العنصر	زيادة الثقة	زيادة استعداد مشاركة البيانات	معدل التطبيق
الشفافية في استخدام البيانات	+38%	+70%	65%
خيارات الاشتراك/عدم الاشتراك	+42%	+42%	80%
تبادل القيمة الواضح	+45%	+72%	55%
التوعية الأمنية المستمرة	+35%	+28%	40%
إظهار الشهادات والامتثال	+52%	+48%	70%
الإشعارات الاستباقية	+40%	+35%	60%

جدول15 تأثير عناصر التسويق الأمني على ثقة العملاء

المصدر:(The Financial Brand, 2024; Thales Group, 2025)

4.3 الحملات التسويقية والإعلانات بالتسويق الأمني

تُمثل الحملات التسويقية والإعلانات الموجهة للتوعية بالأمن الإلكتروني في تطبيقات الدفع الإلكتروني عنصراً استراتيجياً محورياً في بناء ثقة المستخدمين وتعزيز معدلات التبني للخدمات المالية الرقمية على المستوى العالمي. في ظل تصاعد التهديدات السيبرانية وتعقّد أساليب الاحتيال الإلكتروني، استثمرت المؤسسات المالية

الكبرى والشركات التقنية العالمية مليارات الدولارات في تطوير استراتيجيات توعوية شاملة تهدف إلى تعزيز الوعي الأمني لدى المستخدمين وحماية البيانات المالية.(Mastercard, 2024; Visa, 2025)

4.3.1 حملة" Visa ابقَ آمناً :(Stay Secure) "النموذج الرائد في الشرق الأوسط وشمال أفريقيا

الشكل 8 يظهر إحدى إعلانات الحملة

تُعتبر حملة" Visa ابقَ آمناً (Stay Secure) "من أبرز الحملات التوعوية السنوية الشاملة على المستوى الإقليمي، حيث تستهدف المستهلكين في منطقة الشرق الأوسط وشمال أفريقيا بشكل خاص. تعتمد الحملة على استراتيجية تسويقية متعددة القنوات تشمل منصات التواصل الاجتماعي(فيسبوك، إنستغرام، LinkedIn) والإعلانات المطبوعة والرقمية، بالإضافة إلى شراكات مع المؤسسات المالية المحلية (). تركز الحملة على ثلاثة محاور رئيسية: أولاً، التوعية بممارسات الحماية الأساسية مثل عدم مشاركة بيانات البطاقات مع الآخرين والحفاظ على سرية المعلومات الشخصية؛ ثانياً، التعريف بآليات الحماية المتقدمة مثل تقنيات الترميز

(Tokenization)والمصادقة البيومترية وأنظمة الحماية متعددة العوامل؛ وثالثاً، تمكين المستهلكين من التعرف على محاولات الاحتيال والاستجابة المناسبة لها.(Visa Middle East, 2024)

حققت حملة Visa نتائج ملموسة وقابلة للقياس الكمي. كشفت الدراسة التاسعة للحملة أن 97% من المستهلكين عبر الأسواق المستهدفة اتخذوا تدابير احترازية حول المدفوعات الرقمية، بزيادة من 92% في عام 2023، وأن 76% يثقون في المدفوعات الرقمية بشكل كامل أو كبير (Visa, 2025).

الشكل 9 يظهر جزء من حملة ابق آمناً على الموقع الرسمي Visa.com

على المستوى القُطري، أظهرت النتائج أن 96% من المستهلكين في مصر و99% في الإمارات العربية المتحدة و85% في عمان يتخذون خطوات استباقية لحماية معاملاتهم الرقمية (Visa Middle East, 2024). وعلى مستوى الحماية الفعلية، نجحت Visa في حجب أكثر من 40 مليار دولار أمريكي من القيمة الاحتيالية ومنع 80 مليون معاملة احتيالية خلال عام واحد، بالإضافة إلى الحيلولة دون وقوع أكثر من 122 مليون دولار من خسائر الاحتيال الإلكتروني من خلال الكشف عن البرمجيات الخبيثة (Tech Cabal, 2025). يدعم هذا الأداء استثمار طويل الأمد قدره 3.3 مليار دولار في البنية التحتية للذكاء الاصطناعي والبيانات خلال العقد الماضي (Financial IT, 2025).

4.3.2 حملة :"Pay the Apple Way" Apple التركيز على الأمان كميزة تنافسية

أطلقت شركة Apple في عام 2023 حملة تسويقية واسعة النطاق تحت عنوان "Pay the Apple Way" لتعزيز استخدام خدمةApple Pay ، مع التركيز الشديد على الأمان والخصوصية كميزات تنافسية رئيسية (Marketing Dive, 2023). تضمنت الحملة إعلانات خارجية (لوحات إعلانية)، ومحتوى على وسائل التواصل الاجتماعي، وشراكات مع منشئي المحتوى علىTikTok ، مع التأكيد على استخدام تقنية الترميز (Tokenization) التي تضمن عدم مشاركة رقم البطاقة الائتمانية الفعلي مع التجار، بالإضافة إلى المصادقة البيومترية(Face IDوTouch ID) (Apple Newsroom, 2023).

الشكل 10 إعلان لحملة Apple

حققت الحملة نتائج نمو ملحوظة، حيث نما اعتماد Apple Pay بنسبة 41% بين عامي 2022 و2024، ليصل عدد المستخدمين النشطين في الولايات المتحدة إلى 60–65 مليون مستخدم في عام 2025، مع حصة سوقية تبلغ 54% من معاملات المحافظ الرقمية داخل المتاجر(SQ Magazine, 2025). وعلى المستوى المالي، انفجرت إيرادات Apple Pay من 998 مليون دولار في عام 2019 إلى ما يُقدر بـ 4.23 مليار

دولار لعام 2024 و4.45 مليار دولار متوقعة لعام 2025 (Electro IQ, 2025). كما عالج Apple Pay 12%من معاملات البطاقات عبر الإنترنت عالمياً في عام 2023، و14.2% من جميع مدفوعات المستهلكين عبر الإنترنت في عام 2024 (Crop Ink, 2025).

4.3.3 حملة "Surakshit Vyapari, Safal Vyapar" Mastercard التوعية الموجهة للتجار في الهند

أطلقت Mastercard بالتعاون مع اتحاد تجار الهند (CAIT) حملة وطنية في الهند تحت عنوان "Surakshit Vyapari, Safal Vyapar"(التاجر الآمن، التجارة الناجحة) خلال شهر التوعية بالأمن السيبراني في أكتوبر 2024(Mastercard, 2024). تهدف الحملة إلى تدريب التجار الصغار والمتوسطين على كيفية الوقاية من الهجمات الإلكترونية والاحتيال من خلال ورش عمل ودورات تدريبية متخصصة في 29 ولاية هندية (UNI India, 2025).

الشكل 11 من تدريب شركة Mastercard للتجار في الهند

تأتي هذه الحملة استجابة لزيادة بنسبة 300% في حالات الاحتيال الإلكتروني في المدفوعات بالهند، حيث بلغت حوالي 36,000 حالة في السنة المالية 2023 وفقاً للبنك الاحتياطي الهندي. وعلى مدى عقد من التعاون بين Mastercard وCAIT، تم تغطية أكثر من 10 ملايين تاجر، مع استفادة مباشرة لـ 2.5 مليون تاجر من تبني المدفوعات الرقمية (Mastercard, 2024). وقد حددت Mastercard هدفاً طموحاً لتخفيض معدل النقر على محاولات التصيد الاحتيالي إلى 1% عبر المؤسسة، وقد اقتربت من تحقيق هذا الهدف (ASIS International, 2020).

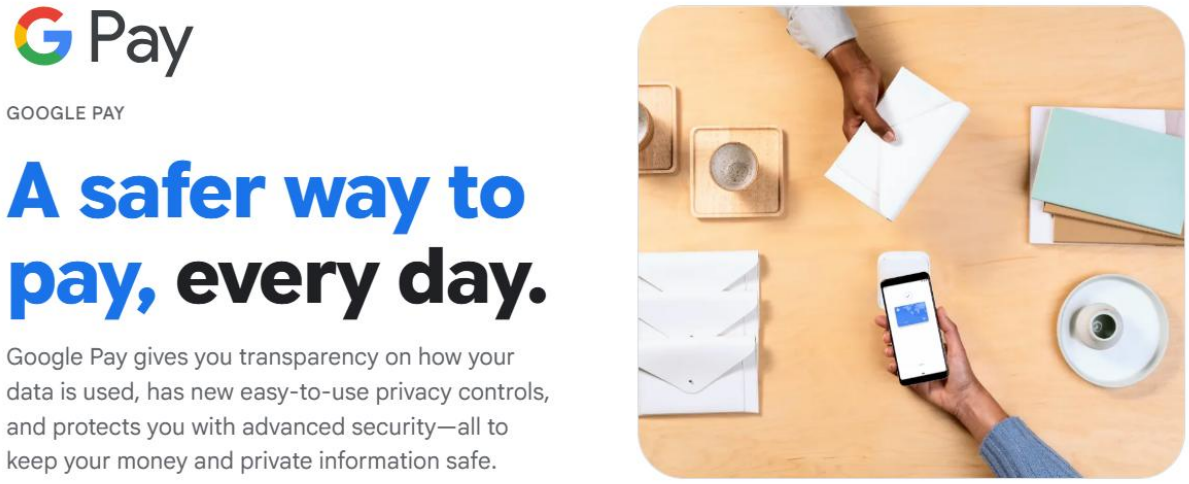
4.3.4 حملة :JPMorgan Chase أكبر مبادرة لمنع الاحتيال في تاريخ المؤسسة

يُعتبر JPMorgan Chase رائداً عالمياً في مجال الوقاية من الاحتيال المالي، حيث أطلق في عام 2024 أكبر مبادرة لمنع الاحتيال والخداع في تاريخ المؤسسة. نجح البنك في حماية عملائه من خسارة 12 مليار دولار أمريكي في محاولات الاحتيال والخداع خلال عام 2024 فقط، مع استثمار سنوي يُقدر بمليارات الدولارات في التقنيات والاستراتيجيات المتطورة لحماية العملاء (JPMorgan Chase, 2025).

تتضمن المبادرة تطوير فريق مقاطعة الخداع المتخصص الذي يعمل بواسطة علماء نفس سلوكيين ومحققين وباحثين في منع الخداع العالمي لإيقاف عمليات الخداع في الوقت الفعلي، بالإضافة إلى استضافة أكثر من 20 ورشة عمل تعليمية مجانية في جميع أنحاء الولايات المتحدة خلال أسبوع التوعية بالاحتيال الدولي بالتنسيق مع الشرطة المحلية (Finextra, 2025). كما تشمل المبادرة تقنيات متقدمة مثل التحذيرات الذكية داخل التطبيق عند اكتشاف أنشطة مشبوهة، وميزة جهة الاتصال الموثوقة التي تسمح للعملاء بتعيين شخص موثوق

لإخطاره بمعاملات معينة، وتدريب BankSafe من AARP لتدريب موظفي الفروع على مساعدة وحماية العملاء خاصة كبار السن (Washington Informer, 2025).

4.3.5 مبادرات Google Pay و PayPal في التوعية الأمنية



الشكل 12 من مبادرة GOOGLE PAY

يوفر Google Pay تدابير أمنية متعددة تشمل التشفير من طرف إلى طرف (End-to-End Encryption)، والترميز (Tokenization) ، والمصادقة الثنائية(2FA) ، والمصادقة البيومترية، ومراقبة النشاط في الوقت الفعلي، مع التركيز في استراتيجيات التوعية على تثقيف المستخدمين حول تجنب هجمات التصيد الاحتيالي والبرمجيات الخبيثة (Bright Defense, 2025). أما PayPal، فقد أطلقت حملات تحذيرية خلال شهر التوعية بالأمن السيبراني الوطني في الولايات المتحدة لتنبيه المستخدمين من عمليات

التصيد الاحتيالي، خاصةً تلك التي تستخدم عناوين بريد إلكتروني شرعية من PayPal لإرسال فواتير وهمية (KnowBe4, 2019; Hoxhunt, 2021).

الشكل 13 من موقع PayPal

4.3.6 المنصات الصينية Alipay وWeChat Pay:

تُعتبر Alipay و WeChat Pay من أكبر منصات الدفع الإلكتروني في العالم، حيث تسيطران على أكثر من 90% من سوق المدفوعات الرقمية في الصين، مع أكثر من 3.5 تريليون دولار في المعاملات السنوية (CoinLaw, 2025). تشمل تدابير الأمان المُعلن عنها: التشفير المتقدم عالي المستوى لحماية جميع المعاملات والبيانات الشخصية، والمصادقة البيومترية باستخدام التعرف على الوجه وبصمة الإصبع، والكشف

التلقائي عن الاحتيال عبر أنظمة ذكية لرصد الأنشطة المشبوهة وإيقافها تلقائياً. ومع ذلك، تخضع المنصتان لتنظيم صارم من السلطات الصينية بشأن حماية البيانات والأمن المالي (Mobile Wallet Cards, 2025).

5. تجربة المستخدم في التطبيقات المالية الرقمية

5.1 أسس تصميم تجربة المستخدم

5.1.1 مفهوم تجربة المستخدم وأهميتها

تُعرّف تجربة المستخدم (User Experience – UX) بأنها المجموع الكلي للتفاعلات والمشاعر والتصورات التي يختبرها الشخص عند استخدام منتج أو خدمة رقمية (ebankit, 2024). في سياق التطبيقات المصرفية عبر الهاتف المحمول، تشمل تجربة المستخدم كل جانب من جوانب تفاعل المستخدم مع التطبيق، من سهولة التنقل ووضوح الواجهة إلى سرعة الاستجابة والأمان المدرك (McKinsey, 2025).

تكتسب تجربة المستخدم أهمية بالغة في التطبيقات المالية نظراً لتأثيرها المباشر على ثقة العملاء واستعدادهم لاستخدام التطبيق (ebankit, 2024). يمكن أن تؤدي مشكلات التصميم أو سهولة الاستخدام البسيطة إلى الإضرار بثقة المستهلك في التطبيق المصرفي. على العكس من ذلك، يمكن للتطبيق المصمم بعناية والذي يتفوق في تجربة المستخدم أن يجذب العديد من العملاء نحو طريقة أكثر ملاءمة للخدمات المصرفية (ebankit, 2024).

5.1.2 مبادئ تصميم تجربة المستخدم

تستند تجارب المستخدم الفعالة في التطبيقات المصرفية إلى عدة مبادئ أساسية:

1. التصميم المتمحور حول المستخدم (User-Centered Design)

يجب أن تضع احتياجات المستخدمين في صميم عملية التصميم. يتطلب ذلك فهماً عميقاً لسلوكيات المستخدمين واحتياجاتهم ونقاط الألم لديهم، مما يمكّن من إنشاء تجربة مصرفية عبر الهاتف المحمول تلبي تفضيلاتهم حقاً وتعزز الرضا العام (ebankit, 2024).

2. البساطة والوضوح

تُعد واجهة نظيفة وبديهية حجر الزاوية لتجربة مصرفية رائعة عبر الهاتف المحمول. نظراً لمحدودية مساحة الشاشة، يجب على البنوك تحديد أولويات الميزات الأكثر استخداماً مثل أرصدة الحسابات والمعاملات الأخيرة وأدوات إعداد الميزانية. تعزز الواجهات الشفافة التي تعرض بوضوح تفاصيل المعاملات، بما في ذلك التصنيف وسمات التاجر، ثقة المستخدم وتسهل التنقل (Snowdrop Solutions, 2025).

3. التخصيص (Personalization)

يدعم المصممون بشدة تنفيذ تجارب مُخصصة تلبي تفضيلات وسلوكيات المستخدمين الفرديين. من خلال دمج التخصيص، يصبح من الممكن تعزيز تفاعل المستخدم وإنشاء تجربة مصرفية عبر الهاتف المحمول ليست ممتعة فحسب، بل ذات مغزى للمستخدم أيضاً (ebankit, 2024).

4. الأمان المدمج (Security by Design)

يجب أن يكون الأمان جزءاً أساسياً من تصميم تجربة المستخدم دون أن يُضر بسهولة الاستخدام. على سبيل المثال، يسمح حل ebankIT للمستخدمين باختيار قناتهم المفضلة لتلقي كلمة المرور لمرة واحدة (OTP) للتحقق من المعاملات، مع ملء تلقائي عند اختيار تلقيها عبر الرسائل النصية القصيرة. يوفر التطبيق المحمول أيضاً المصادقة البيومترية للتخلص من المهمة التي تستغرق وقتاً طويلاً لملء أسماء المستخدمين وكلمات المرور (ebankit, 2024).

المبدأ	الوصف	أمثلة تطبيقية	التأثير على التبني
البساطة	واجهة نظيفة وبديهية	-أيقونات واضحة -قوائم مبسطة -تدفق منطقي	+35%
الوضوح	معلومات شفافة ومفهومة	-عرض الرصيد بوضوح -تفاصيل المعاملات -تسميات دقيقة	+28%
السرعة	استجابة سريعة	-تحميل فوري -معاملات سريعة -تحديث تلقائي	+42%

المبدأ	الوصف	أمثلة تطبيقية	التأثير على التبني
التخصيص	تجربة مُصممة للفرد	–لوحة تحكم قابلة للتخصيص –إشعارات مُخصصة –توصيات ذكية	+30%
إمكانية الوصول	مناسبة لجميع المستخدمين	–دعم قراء الشاشة –تباين الألوان –حجم خط قابل للتعديل	+18%

جدول 16 مبادئ تصميم تجربة المستخدم وتطبيقاتها

5.1.3 تأثير تجربة المستخدم على التبني

تؤثر تجربة المستخدم بشكل مباشر على معدلات تبني التطبيقات المالية واستمرارية استخدامها (McKinsey, 2025). أظهرت دراسة أجرتها Forrester عام 2024 أن بنك BBVA احتل المرتبة الأولى في مراجعة التجربة الرقمية الأوروبية لتطبيقه المحمول بفضل تجربة المستخدم الممتازة وأدوات المالية الاستباقية والإشعارات المُخصصة (Maze, 2025). ساعدت واجهة المستخدم الحوارية والرؤى في الوقت الفعلي لـ BBVA على تبسيط المهام المعقدة مثل تحويل الأموال والادخار والوصول إلى دعم العملاء، مما أكسبه مكانة عليا بين تطبيقات الخدمات المصرفية عبر الهاتف المحمول (Maze, 2025).

تشير البيانات إلى أن الشفافية تقلل بشكل كبير من معدلات توقف العملاء في التطبيقات المصرفية، مما يسلط الضوء على دورها في الولاء على المدى الطويل للعملاء. من خلال تقديم تخطيط منظم وجذاب بصرياً، يمكن للبنوك تعزيز رضا المستخدمين ومعدلات الاحتفاظ بهم بشكل كبير (Snowdrop Solutions, 2025).

5.2 التوازن بين الأمان وسهولة الاستخدام

5.2.1 التحدي المزدوج

يمثل تحقيق التوازن المناسب بين الأمان القوي وتجربة المستخدم السلسة أحد أكبر التحديات في تصميم التطبيقات المالية (ebankit, 2024; Thales Group, 2025). من ناحية، تتطلب الطبيعة الحساسة للمعاملات المالية والبيانات الشخصية تطبيق إجراءات أمنية صارمة لحماية العملاء من الاحتيال والاختراقات (Thales Group, 2025). من ناحية أخرى، يمكن أن تؤدي الإجراءات الأمنية المعقدة أو المرهقة إلى إحباط المستخدمين وتقليل معدلات التبني والاستخدام (ebankit, 2024).

تُظهر الأبحاث أن العملاء يعطون الأولوية للمعلومات الموثوقة (61%) بدرجة أكبر بكثير من سرعة التفاعل (46%) أو الراحة (44%) (The Financial Brand, 2024).هذا يشير إلى أن المستخدمين على استعداد لقبول بعض التعقيد الإضافي إذا شعروا بأن معلوماتهم محمية بشكل كافٍ. ومع ذلك، يجب تصميم هذه الإجراءات الأمنية بطريقة تقلل من الاحتكاك وتحافظ على تجربة مستخدم إيجابية (ebankit, 2024).

العامل	نسبة الأهمية	التصنيف
معلومات موثوقة وآمنة	61%	1
سهولة الاستخدام	54%	2
سرعة التفاعل	46%	3
الراحة	44%	4
التخصيص	38%	5
التصميم الجذاب	32%	6

جدول17 أولويات العملاء في التطبيقات المالية

المصدر:(The Financial Brand, 2024)

5.2.2 استراتيجيات تحقيق التوازن

توجد عدة استراتيجيات لتحقيق التوازن الأمثل:

1. المصادقة التكيفية (Adaptive Authentication)

تستخدم هذه التقنية الذكاء الاصطناعي لتقييم مستوى المخاطر لكل معاملة في الوقت الفعلي، وتطلب مستويات مختلفة من المصادقة بناءً على ذلك (ebankit, 2024). على سبيل المثال:

- معاملات منخفضة المخاطر :مصادقة بسيطة (كلمة مرور أو بصمة).
- معاملات متوسطة المخاطر: مصادقة ثنائية (كلمة مرور+ OTP).
- معاملات عالية المخاطر: مصادقة متعددة (كلمة مرور + OTP + بيومترية).

هذا يوفر المصادقة التي تربط إلى محرك قواعد سيطلب المصادقة فقط عند الضرورة، اعتماداً على المخاطر التي يحددها البنك للمعاملة، مما يضمن تجربة مستخدم سلسة (ebankit, 2024).

2. المصادقة البيومترية

تقدم تقنيات مثل بصمة الإصبع والتعرف على الوجه مستوى عالٍ من الأمان مع تجربة مستخدم سلسة للغاية (ebankit, 2024; Fintech Strategy, 2024). بدلاً من تذكر كلمات مرور معقدة أو إدخال رموز متعددة، يمكن للمستخدمين ببساطة استخدام خصائصهم البيومترية للوصول إلى حساباتهم أو التحقق من المعاملات، مما يجمع بين الأمان القوي والراحة الفائقة.

3. التصميم الأمني الشفاف

بدلاً من إخفاء الإجراءات الأمنية، يجب توضيحها للمستخدمين بطريقة تعزز الثقة دون التسبب في القلق (Thales Group, 2025). على سبيل المثال، يمكن عرض إشعارات بسيطة تخبر المستخدمين بأن

معاملاتهم يتم تشفيرها أو أن نشاطهم يتم مراقبته لاكتشاف الاحتيال، مما يطمئنهم دون إزعاجهم بتفاصيل تقنية معقدة.

4. التبسيط التدريجي (Progressive Disclosure)

يمكن تصميم عمليات الإعداد والتسجيل بطريقة تدريجية، حيث يتم جمع المعلومات الأساسية فقط في البداية، ثم طلب معلومات أمنية إضافية تدريجياً مع زيادة استخدام المستخدم للتطبيق (Didit, 2024). هذا يقلل من حاجز الدخول ويجعل العملية الأولية أكثر سلاسة.

الاستراتيجية	مستوى الأمان	سلاسة الاستخدام	تعقيد التطبيق	معدل القبول
المصادقة التكيفية	عالٍ جداً	عالية	مرتفع	75%
المصادقة البيومترية	عالٍ جداً	عالية جداً	متوسط	85%
التصميم الأمني الشفاف	متوسط–عالي	عالية	منخفض	90%
التبسيط التدريجي	متوسط	عالية جداً	متوسط	80%
MFA التقليدي	عالٍ جداً	متوسطة	منخفض	65%

جدول 18 مقارنة بين استراتيجيات الموازنة بين الأمان والاستخدام

الفصل الثاني

الدراسة العملية

مقدمة:

يهدف هذا القسم إلى ترجمة النظريات إلى واقع قابل للملاحظة والقياس، مما يوفر أساساً متيناً لفهم كيفية تأثير العوامل المختلفة على تبنّي تطبيقات الدفع الإلكتروني في السياق السوري، وتقديم توصيات عملية يمكن للشركات تطبيقها بشكل مباشر.

1. الدراسة الكمية

- أداة الجمع :استبانة إلكترونية منظمة: تم كتابة استبانة البحث عبر ثلاث مراحل رئيسية:

المرحلة الأولى: التخطيط والتصميم الأولي, حيث تم استعراض لأدبيات أكاديمية متعلقة بتبني التكنولوجيا والأمان والثقة. بناءً على هذا الاستعراض، تم تحديد المتغيرات الرئيسية وأبعادها، وصياغة 25 سؤالاً موزعاً على 7 أقسام (البيانات الديموغرافية 4 أسئلة، أمان التطبيق 4 أسئلة، الحملات التسويقية 4 أسئلة، تعقيد الإجراءات 4 أسئلة، ثقة العملاء 4 أسئلة، تبني التطبيق 4 أسئلة، وسؤال مفتوح 1). كل سؤال في الاستبانة تم اختياره بعناية ليس عشوائياً، وتم ربطه بفرضية محددة من فرضيات الدراسة الخمسة. على سبيل المثال، تم تصميم أسئلة محور الأمان المدرك (الأسئلة 5–8) لقياس أربعة أبعاد مختلفة: حماية البيانات الشخصية، الإشعارات الفورية، المصادقة الثنائية، والحماية من الاحتيال، وكل بُعد مشتق من نماذج نظرية معروفة وأدبيات حديثة.

المرحلة الثانية: التحكيم و التطوير: بالبداية تمت كتابة أسئلة استبانة و نشرها على عدد محدود من الأقارب والأصدقاء لتبيان مدى وضوح الأسئلة وسهولة فهمها, وقد جاءت بعض الإجابات خاصة من الأشخاص غير ذوي الخبرة التقنية بأن بعض المصطلحات غير مفهومة, كمصطلح (المصادقة الثنائيةFA2) مما استدعى لإعادة كتابة الأسئلة بشكل واضح ومفهوم من جميع المستخدمين والابتعاد عن المصطلحات التقنية البحتة. ومن ثم تم إرسال الاستبانة للدكتور المشرف حيّان ديب حيث قدّم ملاحظة قيّمة حول أن تكون الاستبانة تتمحور حول تطبيق محدد من تطبيقات الدفع الإلكتروني. وقد تم التعديل بناءً على الملاحظة وأخذ الموافقة بالمباشرة بمرحلة النشر.

المرحلة الثالثة: اختبار الموثوقية والصدق. تم إجراء اختبار موثوقية الاستبانة (Reliability Test) باستخدام برنامج SPSS من خلال تطبيقها على عينة استطلاعية بسيطة (50 مستجيب)، حيث تم حساب معامل كرونباخ ألفا لكل محور وللاستبانة الكاملة. أظهرت النتائج معاملات ثبات عالية جداً (تتراوح بين 0.704 و0.892)، مما يعكس اتساقاً داخلياً قوياً وموثوقية عالية في القياس.

- عدد الاستجابات الأولية: 212 استجابة
- عدد الاستجابات المقبولة: 186 استجابة(87.7%) حيث تم حذف إجابات من لم يستخدم التطبيق مسبقاً لتركيزنا على المستخدمين الحاليين للتطبيق.
- تم استخدام برنامج SPSS وأداة " Hayes Process" (Hayes, 2025) للحصول على التحليلات المطلوبة وبالتالي للإجابة على أسئلة البحث.

2. الدراسة النوعية

- أداة الجمع :مجموعات تركيز (Focus Groups) : تم تطوير دليل أسئلة مجموعات التركيز من خلال عملية منهجية متعددة الخطوات استمرت 7 أيام وكانت على عدة مراحل:

  - المرحلة الأولى: التخطيط والمحاذاة. تم ربط أسئلة مجموعات التركيز مباشرة بأسئلة الاستبانة. كل سؤال من الأسئلة الخمسة عشر الرئيسية تم تصميمه لمناظرة محور معين من محاور الاستبانة (3 أسئلة لكل محور)، بحيث تكمل أسئلة التركيز الأسئلة الكمية بإضافة العمق والسياق والتفاصيل التي لا يمكن جمعها من الاستبانة.
  - المرحلة الثانية: تمت صياغة جميع الأسئلة بشكل مفتوح النهاية (Open-ended)، حيث تم تجنب الأسئلة المغلقة (نعم/لا) والأسئلة المركبة التي تجمع بين فكرتين. كل سؤال تم صياغته بحيث يسمح للمشاركين بـ الإجابة بحرية كاملة وليس فقط الموافقة أو عدم الموافقة على عبارات محددة. على سبيل المثال، بدلاً من قول "هل أنت مقتنع بأمان التطبيق؟"، تم صياغة السؤال كـ "ما الذي يجعلك تشعر بالأمان عند استخدام التطبيق؟ وما الذي قد يقلقك؟"، وهذا يسمح بإجابات متنوعة وغنية. تم أيضاً بناء تسلسل منطقي يبدأ من الأسهل والأكثر راحة (التعريف والتجربة الأولى) ثم ينتقل تدريجياً للأسئلة الأكثر عمقاً والحساسة (المخاوف، الاقتراحات).
  - المرحلة الثالثة: الاختبار والتحسين: تم اختبار الأسئلة على مجموعة استكشافية صغيرة (جلسة تجريبية مع 6 مشاركين)، حيث تم ملاحظة وقت الجلسة، وضوح الأسئلة، وعمق الإجابات.

بناءً على الملاحظات، تم تعديل صياغة 4 أسئلة لتوضيح المقصود، وإضافة أسئلة توضيحية فرعية لكل سؤال رئيسي (مثل: "هل يمكنك شرح ذلك أكثر؟"، "هل يمكنك إعطاء مثال محدد؟")، وإعادة ترتيب ترتيب الأسئلة قليلاً لضمان تدفق أفضل.

- عدد المجموعات: 4 مجموعات تركيز
- عدد المشاركين في كل مجموعة: 6–8 مشاركين
- إجمالي المشاركين: 28 مشاركاً
- التحليل :تحليل موضوعي لاستخلاص الرؤى

و قد كان هيكل جلسات مجموعات التركيز كما في الجدول(19):

رقم المرحلة	عنوان المرحلة	مدة المرحلة	رقم السؤال	الهدف
الأولى	الترحيب والتعارف	**10 دقائق**	1	– كسر الجليد –التعرف على المشاركين –فهم مستوى خبرتهم بالتطبيق –بناء جو من الراحة والثقة

الثانية	أسئلة التمهيد والإحماء	**10 دقائق**	2	–فهم دوافع التبني الأولية –معرفة مصادر المعلومات (إعلانات، أصدقاء، عائلة) –استكشاف الانطباعات الأولى –الربط بـ الاستبانة
الثالثة	أسئلة الاستكشاف الرئيسية حسب المحاور	**40- 50 دقيقة**	3-17	–كشف المخاوف الحقيقية غير المعبّر عنها –الحصول على قصص وتجارب حقيقية –فهم المواقف التي تبني أو تضعف الثقة –تقييم الميزات الحالية –الحصول على اقتراحات تحسين مباشرة من المستخدمين –فهم الفجوات بين التوقعات والواقع –أهداف أخرى (تم ذكرها بالملحق)
الرابعه	أسئلة التعمق والتفصيل	**15 دقيقة**	18	–استخلاص أهم أولويات التحسين من وجهة نظر المستخدمين

				-الحصول على توصيات محددة وقابلة للتنفيذ 19-ترتيب الأولويات حسب أهميتها -الحصول على رؤى يمكن مشاركتها مع فريق التطوير
الخامسة	الختام والتوصيات	**10 دقائق**	19	-التقاط أي رؤى إضافية لم تُغطَّ -إعطاء المشاركين فرصة أخيرة للمساهمة -اكتشاف مواضيع لم نفكر فيها مسبقاً -ضمان عدم ترك أي نقطة مهمة

جدول 19 هيكل جلسات مجموعات التركيز

3. النتائج الرئيسية

3.1 خصائص العينة والسوق المستهدف

الخاصية	النتيجة	الآثار الإدارية
الجنس	ذكور 65.1%، إناث 34.9%	توازن جيد، لا حاجة لحملات منفصلة
العمر	95.7%في الفئة 20–49 سنة	التركيز على الفئات النشطة اقتصادياً
التعليم	+60%جامعي فأعلى	استهداف متعلم ومثقف تقنياً

جدول20 خصائص العينة والسوق المستهدف

رأي الباحث: العينة تمثل السوق السوري حيث أن معظم المشاركين من فئة الشباب (20–49) الأكثر استخداماً للتطبيقات والتكنولوجيا، كما أن التوازن بين عدد الذكور والإناث كان توازناً جيداً.

3.2 التحقق من صدق وثبات أداة الدراسة

المحور	ألفا كرونباخ
أمان التطبيق	.774
الحملات التسويقية	.841
تعقيد الإجراءات	.766
ثقة العملاء	.836
تبني التطبيق	.892

جدول 21 التحقق من صدق وثبات أداة الدراسة

من الجدول السابق نلاحظ درجة ثبات جيدة إلى عالية لجميع المحاور.

3.3 التحقق من قياس صحة المحاور والاتساق الداخلي

المحور	المتوسطات الحسابية	Sig.
أمان التطبيق	بين 3.44 و 3.9	.000
الحملات التسويقية	بين 3.5 و 3.74	.000

تعقيد الإجراءات	بين 2.23 و 2.97	.000
ثقة العملاء	بين 3.77 و 3.87	.000
تبني التطبيق	بين 3.66 و 4.03	.000

جدول22 التحقق من قياس صحة المحاور والاتساق الداخلي

من الجدول السابق نجد أن الأسئلة ضمن المحور الواحد متسقة مع بعضها أي أن الأسئلة لا تقيس مواضيع مختلفة.

3.4 مستويات الإدراك والثقة الحالية

المتغير	المتوسط	التقييم	نتيجة مجموعات التركيز
أمان التطبيق	3.66	إيجابي معقول	الإشعارات والرموز مقدّرة، لكن مخاوف من الاحتيال
الحملات التسويقية	3.62	إيجابي معقول	تركز على العروض أكثر من الأمان
تعقيد الإجراءات	2.60	منخفض (نقطة قوة)	الشباب لا يشعرون به، الأكبر يحتاجون دعماً
ثقة العملاء	3.82	إيجابي قوي	مبنية على السمعة والخدمة والتجربة

المتغير	المتوسط	التقييم	نتيجة مجموعات التركيز
تبني التطبيق	3.88	مرتفع جداً	منتظم لكن حذر مع المبالغ الكبيرة

جدول 23 مستويات الإدراك والثقة الحالية

3.5 النتيجة الأولى: تأثير الأمان على التبني

Sig.	R Square	β
.000[b]	.378	.615[a]

جدول24 النتيجة الأولى: تأثير الأمان على التبني

الدلالات الإحصائية:

- تأثير مباشر قوي$\beta = 0.615, p < 0.001$:
- الأمان يفسر 37.8% من التباين في قرار التبني
- كل زيادة بمقدار 1 وحدة في الأمان ترتبط بزيادة 0.743 وحدة في التبني

مجموعات التركيز:

- *"الإشعارات الفورية هي أهم شيء بالنسبة لي. كل ما أعمل عملية، يجيني إشعار فوراً. هذا يطمّنني إنه ما حدا يقدر يستخدم حسابي بدون ما أعرف".*

- *"رمز التحقق اللي بيجي على الموبايل بخليني متطمن. يعني حتى لو حدا عرف كلمة السر، ما بيقدر يدخل بدون موبايلي".*

رأي الباحث:

يمكن تفسير النتائج بأن الأمان هو محرك أساسي لقرار تبني التطبيق وبالتالي يجب أن يكون العنصر الأساسي في الكثير الحملات. وأن الاستثمار في الأمان هو استثمار تسويقي استراتيجي فلا ينبغي النظر إليه كتكلفة تشغيلية فقط.

3.6 النتيجة الثانية: الفروقات حسب الفئة العمرية

المحور	Sig.	F
أمان التطبيق	.380	1.031
الحملات التسويقية	.002	5.275
تعقيد الإجراءات	.051	2.642
ثقة العملاء	.388	1.013
تبني التطبيق	.129	1.916

جدول25 النتيجة الثانية: الفروقات حسب الفئة العمرية

الدلالات الإحصائية:

- فروق معنوية في استجابة الحملات التسويقية $F = 5.275, p = 0.002$
- لا توجد فروق معنوية في الأمان والثقة والتبني حسب العمر

مجموعات التركيز:

- *"الأمان أولاً، خاصة بسوريا. الناس خايفة على مصاريها"*. (مشارك من الفئة 20–29)
- *"أنا بدي أعرف كيف بيحمي التطبيق مصاريي ومعلوماتي. مو بس يقولوا آمن، بدي يشرحوا كيف"*. (مشارك من الفئة 30–39)
- *"بدي أعرف شو بيصير لو ضيعت تلفوني أو انسرق. كيف بقدر أحمي المصاري اللي بالتطبيق؟"*. (مشارك من الفئة 40–49)

رأي الباحث:

يرى الباحث أن فرق الاستجابة للحملات التسويقية حسب العمر من الممكن أن يكمن بعدة عوامل, كالخبرة التكنولوجية التي تكون أكبر عند الفئات الشابة "20–39" من الفئات الأكبر"أكبر من 40" ممن يحتاجون لرسائل تسويقية أبسط و أكثر وضوح، تشرح الأمان بلغة سهلة الفهم بدلاً من المصطلحات التقنية. أما بالنسبة لعدم وجود فروقات بتعقيد الإجراءات ($p>0.05$) فيمكننا إرجاع السبب إلى أن الإجراءات في التطبيق المدروس سهلة وغير معقدة فلم يكن هناك حاجة لخبرة تقنية واعتياد على التكنولوجيا الموجودة عند فئة معينة دون أخرى.

3.7 النتيجة الثالثة: الحملات التسويقية

	Sig.	β

تأثير الحملات التسويقية على تبني التطبيق	.114	.111

	Pearson Correlation	Sig. (2-tailed)
العلاقة الخطية بين الحملات التسويقية وثقة العملاء	.650**	.000

جدول 26 النتيجة الثالثة: الحملات التسويقية

الدلالات الإحصائية:

- التأثير المباشر على التبني ($\beta = 0.111, p = 0.114$) غير معنوي
- الارتباط مع الثقة قوي جداً $r = 0.650, p < 0.001$
- التأثير غير المباشر عبر الثقة أقوى من التأثير المباشر

مجموعات التركيز:

- *"الكلام من شخص بتعرفه أقوى من أي إعلان".*
- *"قصص من ناس حقيقيين بتأثر فيني أكثر. إذا شخص متلي استخدمه واستفاد، بيشجعني".*

رأي الباحث:

من الممكن أن تكمن المشكلة بندرة أو عدم وجود حملات تسويقية أو إعلانات تشرح مفهوم أوأهمية الأمان بالتطبيق وبالتالي شعر المستجيبون ألا أهمية لها أو أنها لن تساهم بزيادة ثقتهم بالتطبيق وتبنيهم له.

3.8 النتيجة الرابعة: تأثير تعقيد الإجراءات الأمنية

	β	t	Sig.
تأثير تعقيد الإجراءات الأمنية على تبني التطبيق	−.093	−1.798	.074

جدول27 النتيجة الرابعة: تأثير تعقيد الإجراءات الأمنية

الدلالات الإحصائية:

تعقيد الإجراءات له تأثير سلبي على تبني التطبيق($\beta = -0.093, t = -1.798, p = 0.074$) ولكنه غير دال إحصائياً.

مجموعات التركيز:

- *"أنا بشوف إنو التعقيد مو مشكلة، العكس! لما أشوف خطوات كتيرة، بحس إنو تطبيقهم آمن ومهتم بالأمان. بس المشكلة إذا الإنترنت بطيء، والخطوات كتيرة، بتطول العملية وبتصير مملة."*
- *"أنا شايف إنو التعقيد مقبول. المشكلة الحقيقية إذا نسيت رمز PIN مابعرف وقتها كيف أتصرف أو إذا ماكانت عندك إنترنت قوية... بس الحمدلله، أنا شخصياً متعود. بس لما أحكي مع أصحابي الأكبر مني، بيقولولي إنو كتيرمعقّد وما بيفهموا شي."*

رأي الباحث:

هذه النتيجة قد تعكس حقيقة أن المستخدمين السوريين في العينة قد يكونون قد تكيّفوا بالفعل مع مستوى معين من التعقيد، أو أن التعقيد في نطاق الدراسة لم يصل إلى الحد الذي يُصبح عنده مشكلة بارزة .كما أن الثقة قد تلعب دوراً تعديلياً حيث إذا كان المستخدم يثق بالتطبيق، فقد يتقبل التعقيد كـ "ثمن ضروري للأمان"، وبالتالي لا يؤثر بشكل معنوي على قرار التبني، هذا كما أظهرته دراسة Siagian et al. (2022) في إندونيسيا "أن تأثير التعقيد يختلف حسب مستوى الثقة". من الناحية التطبيقية، هذه النتيجة تطمئن الشركات بأن زيادة إجراءات الأمان المعقولة (كما هي في التطبيق المدروس) لن تدفع المستخدمين للتخلي عن التطبيق، طالما أنها تبقى ضمن حدود المقبولية. لكن يجب الحذر: هذا لا يعني أن التعقيد المفرط أو زيادة خطوات التحقق بشكل مبالغ فيه لن يكون له تأثير سلبي .

3.9 النتيجة الخامسة: دور الثقة كمتغير وسيط

	coeff	se	t	p	LLCI	ULCI
security	.6961	.0516	13.5004	.0000	.5944	.7978

	Effect	BootSE	BootLLCI	BootULCI
trust	.4407	.0695	.3081	.5780

جدول28 النتيجة الخامسة: دور الثقة كمتغير وسيط

الدلالات الإحصائية:

- التأثير الكلي للأمان على التبني: 0.6961
- التأثير غير المباشر عبر الثقة: 0.4407 (63% من التأثير الكلي)
- التأثير المباشر المتبقي: 0.3023 (37%)

مجموعات التركيز:

- *"الثقة بتيجي من التجربة. كل ما استخدمت التطبيق أكثر، ثقتي زادت".*
- *"مرة حولت مبلغ غلط. تواصلت مع خدمة العملاء وساعدوني أرجع المبلغ خلال يومين. هاي الخدمة عطتني ثقة كبيرة".*

رأي الباحث:

هذه النتيجة تقول للشركات بوضوح تام أنه لا يمكن ببساطة بناء تطبيق آمن وتسويقه جيداً والعودة للبيت. بل إن الأمان والحملات التسويقية وحدها غير كافية. يجب أن يشعر المستخدم حقيقة بالثقة وهذا نوع من الشعور النفسي العميق الذي يتطلب استمرارية وعمق وشفافية. الثقة ليست شيئاً يمكن "بيعه" أو "الإعلان عنه"، بل يجب أن يُكتسب عبر التجارب الإيجابية المتكررة والالتزام طويل الأمد والشفافية الحقيقية والمسؤولية عند حدوث أي مشكلة. ويجب أن تركز على بناء الثقة من خلال القصص مثل: "مئات الآلاف من المستخدمين يثقون بنا منذ 10 سنوات"، الشهادات مثل: "لم نعاني من أي اختراق منذ التأسيس"، الشفافية مثل: "إليك كيف نحمي بياناتك بالتفصيل". وإن تأثير الأمان أو الحملات مباشرة لا يصل مباشرةً للتبنّي، بل يمر عبر الثقة أولاً. هذا يعني أن تحسين الأمان وحده دون بناء الثقة غير كافٍ، الثقة هي" الجسر "الذي يربط بين ما تقدمه

الشركة تقنياً وبين ما يشعر به المستخدم فعلياً، وبدون هذا الجسر، لن يعبر المستخدم نحو التبنّي حتى لو كانت الإشارات التقنية قوية جداً. هذا يفسر لماذا تطبيقات آمنة تقنياً قد تفشل في التبنّي، بينما تطبيقات أقل تطوراً –لكنها اكتسبت ثقة العملاء– تنجح. الفرق ليس التقنية، بل الثقة، وكمثال على أن الثقة أهم من التقنية العالية والأمان ما تم التوصل إليه في دراسة Magaji وآخرون (2025) حيث جاء بها أنّ عملة رقمية لبنك مركزي قد تكون آمنة تقنياً، لكنها تفشل في التبنّي إذا ارتبطت في أذهان المستخدمين بالرقابة الحكومية وانتهاك الخصوصية. في المقابل،جاء في دراسة Mas, Radcliffe (2010) أن نظام M–PESA حقق في كينيا انتشاراً واسعاً رغم اعتماده على بنية تقنية أبسط تعتمد على الرسائل النصيّة، لأنّ Safaricom ركّزت على بناء الثقة في شبكة الوكلاء وربط الخدمة بعلامة تجارية موثوقة، حتى إنّ مؤلفين وصفوا علاقات الثقة بأنّها "شرط مسبق" لاعتماد الخدمة.

4. تلخيص النتائج

1. الأمان المدرك عامل حاسم في التبني:حيث أظهرت النتائج وجود تأثير مباشر قوي للأمان المدرك على تبنّي التطبيق
2. الثقة هي أقوى محدّد للتبني وتعمل كمتغير وسيط: حيث بيّنت النتائج أن الثقة تملك تأثيراً قوياً جداً على التبني، كما ظهر أن تأثير الأمان والحملات التسويقية ينتقل بدرجة كبيرة عبر الثقة، وليس مباشرة نحو التبنّي.
3. الحملات التسويقية تؤثر بشكل غير مباشر عبر الثقة: حيث أن دور الحملات الرئيس هو بناء الثقة أكثر من دفع التبنّي بشكل مباشر.

4. تعقيد الإجراءات الأمنية تأثيره سلبي ضعيف: ما يشير إلى أن مستوى التعقيد الحالي لا يمثل عائقاً حرجاً لدى غالبية المستخدمين، وإن كان يولّد انزعاجاً لدى بعض الفئات، خصوصاً الأكبر سناً، كما أظهرت مجموعات التركيز.

5. الفروق العمرية تتركز في الاستجابة للحملات التسويقية فقط: حيث بيّنت اختبارات الفروق وجود فروق معنوية في استجابة الفئات العمرية للحملات التسويقية الأمنية، في حين لم تظهر فروق معنوية في إدراك الأمان أو مستوى الثقة أو التبني، ما يعني أن جوهر الرسالة التسويقية واحد، لكن طريقة تقديمها وقنواتها يجب أن تُفصَّل حسب العمر.

5. التوصيات

1. جعل الأمان محور الرسالة التسويقية الأساسية: ينبغي أن يتمحور الخطاب التسويقي حول إبراز عناصر الأمان الواضحة (التشفير، الإشعارات الفورية، المصادقة الثنائية)، مع ترجمتها إلى لغة مبسّطة تصف ماذا يستفيد العميل عملياً من هذه التقنيات (مثل: حماية الرصيد، التنبيه الفوري، الحد من الاحتيال).

2. التركيز على بناء الثقة كهدف تسويقي إستراتيجي: بما أن الثقة تفسّر ما يقارب نصف التبنّي، ينبغي أن تنتقل الحملات من نمط "*نحن آمنون*" إلى نمط "*هذه قصص حقيقية تثبت أننا آمنون وموثوقون*"، وذلك عبر:

- إبراز تاريخ الخدمة وسجلها في حماية أموال العملاء.
- استخدام شهادات حقيقية لمستخدمين من شرائح مختلفة.
- إظهار الشفافية في الرسوم والإجراءات وسياسات حماية البيانات.

3. تصميم حملات مخصَّصة للفئات العمرية: بما أن الفروق العمرية ظهرت فقط في استجابة الحملات، توصى الإدارة التسويقية بتفصيل الرسائل كما يلي:

- الفئة 20–39 سنة :حملات رقمية مكثفة عبر وسائل التواصل الاجتماعي، تستعمل محتوى بصري قصير، ورسائل تركز على السهولة والابتكار مع تضمين رسائل أمان واضحة.
- الفئة 40–49 سنة وما فوق :حملات أكثر هدوءاً وشرحاً (فيديوهات أطول، منشورات توضيحية، ورش تعريفية)، مع التركيز على الضمانات، السمعة، دعم خدمة العملاء، وبساطة الاستخدام خطوة بخطوة.

4. المحافظة على مستوى معقول من الإجراءات الأمنية دون تعقيد مفرط: رغم أن تعقيد الإجراءات لم يظهر كعائق معنوي، إلا أنّ شهادات مجموعات التركيز – خاصة من الفئات الأكبر سناً – تشير إلى أن أي زيادة غير محسوبة في عدد الخطوات قد ترفع مقاومة الاستخدام. يُوصى بالمحافظة على:

- أقل عدد ممكن من الخطوات لتحقيق نفس مستوى الأمان.
- اعتماد الحلول "الخفية" للمستخدم مثل التشفير والترميز، والتركيز على المصادقة البيومترية حيثما أمكن، لتقليل الإدخال اليدوي للرموز.

5. تعزيز التكامل بين الأنشطة التسويقية والقنوات الخدمية: يجب أن تكون الرسالة التي يتلقاها العميل في الإعلان، وفي تجربة التطبيق، وفي تفاعل خدمة العملاء، متسقة ومتناسقة حول محوري الأمان والثقة، بحيث يتحول كل تواصل مع الشركة إلى فرصة لإعادة تأكيد هذه القيم.

6. اقتراحات تطبيقية للشركة:

- إنشاء مرصد دوري لثقة العملاء يقيس الثقة والأمان المدرك كل 6 أشهر، وربطه بمؤشرات التبنّي والاستخدام الفعلي.
- تطوير محتوى تعليمي أمني (مقاطع فيديو قصيرة، كتيبات مبسطة، منشورات توعوية) يشرح بلغة بسيطة سيناريوهات مثل: ماذا يحدث لو ضاع الهاتف؟ كيف أوقف الحساب؟ كيف أحمي كلمة المرور؟
- إطلاق برنامج "سفراء الثقة "يضم عملاء راضين من شرائح مختلفة يشاركون تجاربهم في الوسائل الرقمية والحملات.

6. خطة عمل تسويقية مقترحة

6.1 الهدف العام للخطة

تعزيز تبنّي واستخدام تطبيق الدفع الإلكتروني من خلال بناء ثقة مستدامة لدى العملاء، وتفصيل الحملات التسويقية وفق الفئات العمرية، مع الحفاظ على توازن فعّال بين الأمان وسهولة الاستخدام.

6.2 مراحل الخطة وأنشطتها

أ) المرحلة القصيرة الأجل (0–6 أشهر): بناء الأساس

الأهداف:

- رفع إدراك الأمان والثقة لدى المستخدمين الحاليين والمحتملين.
- تحسين وضوح الرسائل الأمنية في جميع نقاط الاتصال.

الأنشطة الرئيسة:

- مراجعة شاملة لجميع الرسائل التسويقية الحالية، وإعادة صياغتها بحيث:
  - تذكر بوضوح كيف يحمي التطبيق أموال المستخدم وبياناته.
  - تستخدم لغة بسيطة خالية من المصطلحات التقنية المعقدة.
- إنتاج حزمة محتوى أمني تعليمي:
  - 3–5فيديوهات قصيرة (30–60 ثانية) تشرح إجراءات الأمان بشكل مبسط.
  - منشورات توعوية ثابتة (إنفوغرافيك) تُنشر على فيسبوك وإنستغرام.
- تدريب موظفي خدمة العملاء على:
  - أسلوب موحّد لشرح الأمان والثقة.
  - كيفية طمأنة العملاء القلقين من الاحتيال.

- إطلاق استبيان قصير داخل التطبيق لقياس:
  - شعور العميل بالأمان.
  - مستوى الثقة.
  - اقتراحات فورية للتحسين.

ب) المرحلة المتوسطة الأجل (6–12 شهراً): التخصيص والتجزئة

الأهداف:

- تصميم حملات تفصيلية للفئات العمرية المختلفة.
- ترجمة الثقة المتزايدة إلى زيادة فعلية في التبنّي والاستخدام المتكرر.

الأنشطة الرئيسة:

- بناء شرائح عملاء حسب العمر والاستخدام
- للفئة 20–39 سنة:
  - حملات عبر وسائل التواصل (Instagram, TikTok, Facebook) تركز على سهولة الاستخدام، السرعة، والأمان، مع أسلوب بصري حيوي.
  - تشجيع الإحالة (Referral Program) عبر مكافآت صغيرة لمن يدعو أصدقاءه لاستخدام التطبيق.

- للفئة 40:+

  - فيديوهات تعليمية أطول (3–5 دقائق) تشرح التطبيق خطوة بخطوة.
  - ندوات إلكترونية أو جلسات تعريفية بالتعاون مع فروع أو وكلاء.
  - رسائل SMS أو بريد إلكتروني موجه تركز على الضمانات، إجراءات حماية الحساب، وقنوات المساعدة.

- متابعة مؤشرات الأداء الرئيسة:

  - عدد المستخدمين النشطين شهرياً.
  - معدل المعاملات لكل مستخدم.

ج) المرحلة الطويلة الأجل (12–24 شهراً): ترسيخ الثقة وبناء الولاء

الأهداف:

- ترسيخ مكانة التطبيق كخيار أول موثوق للدفع الإلكتروني.
- تحويل الثقة إلى ولاء طويل الأمد وانخفاض في معدلات الهجر.

الأنشطة الرئيسة:

- بناء برنامج ولاء (Loyalty Program) يرتبط:

  - بعدد المعاملات الآمنة المنجزة.

- بسنوات الاستمرارية في استخدام التطبيق.

- نشر تقارير دورية مبسطة (مرة كل 6 أشهر) توضح:
  - عدد محاولات الاحتيال التي تم إيقافها.
  - الإجراءات الجديدة التي تم تطبيقها لتعزيز الأمان.
  - قصص نجاح حقيقية لمستخدمين أو شركاء تجاريين.

- تعزيز الشراكات مع جهات ذات مصداقية عالية (شركات كبرى، جهات تنظيمية)، لإسناد الثقة المؤسسية للتطبيق.

المراجع

المراجع العربية:

النجار، م. ج. (2021). التسويق الإلكتروني. دمشق: الجامعة الافتراضية السورية .

المراجع الأجنبية:

Ajibade, P. (2018). Technology Acceptance Model limitations and criticisms: Exploring the practical applications and use in technology-related studies, mixed-method, and qualitative researches. *Library Philosophy and Practice*.

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health, 26*(9), 1113–1127.

Aljaradat, A., Bani-Khaled, T., & Al-Smadi, A. (2024). Modelling cybersecurity impacts on digital payment adoption. *FinTech, 3*(2), 195–210.

Almaiah, M. A., Alamri, A. M., Al-Zahrani, A., & Almsleh, H. (2022). Factors influencing adoption of digital payment services for bank users: An extended Technology Acceptance Model with trust and risk elements. *Electronics, 11*(23), 3926.

Al-Sharafi, M. A., Arshah, R. A., Abu-Shanab, E. A., & Elayah, N. (2023). The effect of security and privacy perceptions on customers' trust to accept internet banking services: An extension of TAM. *Journal of Engineering Research and Reports, 2*(4), 1–14.

Davis, F. D. (1989a). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989b). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003.

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, 38*(3), 475–487.

Doerr, S., Gambacorta, L., Guibaud, S., & Lopez Forero, A. (2023). Privacy regulation and fintech lending. *BIS Working Papers, 1103*.

Eksteen, C., & Humbani, N. (2021). Understanding proximity mobile payments adoption in South Africa. *Journal of African Business, 22*(3), 344–365.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90.

Granić, A. (2022). Educational technology adoption: A systematic review. *Education and Information Technologies, 27*(7), 9725–9744.

Han, S. (2003). Individual adoption of information systems in organizations: A literature review of Technology Acceptance Model. *Turku Centre for Computer Science Technical Report, 569*.

Hossain, M. (2019). Assessing technology adoption barriers to mobile payment services: A case study of Bangladesh. *Journal of Management Information Systems Research, 15*(2), 145–168.

Jafri, J. A., Wan-Hussin, W. N., & Abdul-Latif, H. I. (2023). A systematic literature review of the role of trust and security on Fintech adoption in banking. *Heliyon, 10*(1), e22980.

Kapoor, A., & Sindwani, M. (2021). Mobile wallet adoption intention amid COVID-19 pandemic: A mediated-moderation framework. *Journal of Electronic Commerce Research, 22*(2), 78–103.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359.

Siagian, H., Cahyono, Y., Purwanto, A., & Suharto, S. (2022). Effect of cybersecurity awareness and organizational culture on technology adoption. *Journal of Theoretical and Applied Information Technology, 100*(4), 1234–1248.

Stewart, H., & Jörjens, J. (2018). FinTech in Europe: Current landscape and future perspectives. In *Handbook of blockchain, digital finance, and inclusion* (Vol. 2, pp. 245–268). Academic Press.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342–365.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273–315.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 17*(5), 328–376.

Williams, M. D., Rana, N. P., & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): A literature review. *Journal of Enterprise Information Management, 28*(3), 443–488.

Worthington, A. K. (2021). Technology Acceptance Model. In *Persuasion theory in action*. University of Arkansas Press.

Xue, L., Jiang, C., Chang, S. H., Wang, Q., & Yang, K. (2024). The Unified Theory of Acceptance and Use of Technology (UTAUT) in higher education: A systematic review. *SAGE Open, 14*(1), 1–26.

المراجع من المواقع الإلكترونية:

Akitra. (2025). *Cybersecurity threats to digital payments*. Retrieved from **https://akitra.com/cybersecurity-threats-to-digital-payments/**

AuditBoard. (2025). *NIST vs. ISO: What's the difference?* Retrieved from **https://auditboard.com/blog/nist-vs-iso-whats-the-difference**

Bakkah. (2025). *مخاطر الأمن السيبراني – كيفية تقييم المخاطر السيبرانية [Cyber risk assessment: How to evaluate cyber risks]*. Retrieved from **https://bakkah.com/ar/knowledge-center/how-to-perform-a-cyber-risk-assessment**

Didit. (2024). *الإدماج في التكنولوجيا المالية: أفضل الممارسات لتحسين تجربة المستخدم [Fintech onboarding: Best practices to optimize user experience]*. Retrieved from **https://didit.me/ar/blog/fintech-onboarding-best-practices-to-optimize-user-experience/**

ebankit. (2024). *User experience: 5 UX principles for mobile banking apps*. Retrieved from **https://blog.ebankit.com/blog-press/user-experience-5-ux-principles-for-mobile-banking-apps**

EVERFI. (2025). *5 digital marketing trends in financial services*. Retrieved from **https://everfi.com/blog/financial-education/5-financial-services-marketing-trends/**

Fintech Strategy. (2024). *The growing importance of cybersecurity in digital payments*. Retrieved from **https://www.fintechstrategy.com/blog/2024/08/20/the-growing-importance-of-cybersecurity-in-digital-payments/**

Fully Vested. (2025). *Digital marketing for financial services: Tips, ideas & strategies*. Retrieved from https://fullyvested.com/insights/digital-marketing-for-financial-services/

Hyperproof. (2025). *NIST CSF guide: Cybersecurity risk management*. Retrieved from https://hyperproof.io/nist-cybersecurity-framework/

ISMS Online. (2025). *How to leverage NIST & ISO 27001 for risk management*. Retrieved from https://www.isms.online/iso-27001/risk-management/nist-iso-frameworks/

Landingi. (2025). *Digital marketing for financial services and institutions*. Retrieved from https://landingi.com/digital-marketing/financial-services/

Maze. (2025). *Mobile banking experiences: Trends and best practices*. Retrieved from https://maze.co/collections/finance/mobile-banking-experience/

McKinsey. (2025). *Building a world-class mobile-banking app*. Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/building-a-world-class-mobile-banking-app

Metomic. (2025). *Data security for financial services: How can FinTech companies protect sensitive customer and financial data?* Retrieved from https://www.metomic.io/resource-centre/how-can-fintech-companies-protect-sensitive-customer-and-financial-data

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). Retrieved from https://csrc.nist.gov/projects/risk-management

Neil Patel. (2025). *Getting started with digital marketing for financial services*. Retrieved from https://neilpatel.com/blog/finance-digital-marketing/

OneTrust. (2025). *ISO 27001 vs. NIST Cybersecurity Framework*. Retrieved from https://www.onetrust.com/blog/iso-27001-vs-nist-cybersecurity-framework/

Snowdrop Solutions. (2025). *Mobile-first banking: UX best practices for 2025*. Retrieved from https://snowdropsolutions.com/mobile-first-banking-ux-best-practices-for-2025/

Tech For Good Institute. (2025). *Understanding the role of trust in digital financial services in Southeast Asia*. Retrieved from https://techforgoodinstitute.org/blog/perspectives/understanding-the-role-of-trust-in-digital-financial-services-in-se-asia/

Thales Group. (2025). *Building trust in digital banking: Securing payment experiences*. Retrieved from https://www.thalesgroup.com/en/news-centre/insights/enterprise/financial-services/building-trust-digital-banking-securing-payment

The Financial Brand. (2024). *How building and sustaining trust has become paramount in the digital age*. Retrieved from https://thefinancialbrand.com/news/bank-culture/how-building-and-sustaining-trust-has-become-paramount-in-the-digital-age-182455

Three29. (2025). *Our top 10 digital marketing strategies for financial services*. Retrieved from https://www.linkedin.com/pulse/our-top-10-digital-marketing-strategies-financial-services-three29

Visure Solutions. (2025). *إدارة مخاطر الأمن السيبراني: الأطر وأفضل الممارسات [Cybersecurity risk management: Frameworks and best practices]*. Retrieved from https://visuresolutions.com/ar/

World Bank. (2025). *Cyber risks in fast payment systems*. Retrieved from https://fastpayments.worldbank.org/

Xygeni. (2025). *ما هي إدارة المخاطر في الأمن السيبراني؟ [What is risk management in cybersecurity?]*. Retrieved from https://xygeni.io/ar/sscs-glossary/what-is-risk-management-in-cyber-security/

الملاحق

أولاً: الاستبانة

عزيزي المشارك،

تهدف هذه الاستبانة إلى دراسة أثر عوامل الأمان في تطبيق الدفع الإلكتروني MTN Cash على ثقة المستخدمين وتبنيهم لهذا التطبيق. جميع إجاباتك سرية وتستخدم لأغراض البحث العلمي فقط. نرجو الإجابة على الأسئلة بموضوعية، ولا توجد إجابة صحيحة أو خاطئة

<u>البيانات الديموغرافية</u>

1. الجنس
   - ذكر
   - أنثى
2. العمر
   - أقل من 20
   - بين 20 و 29
   - بين 30 و39
   - بين 40 و49
   - 50 فأكثر
3. المستوى التعليمي:
   - ثانوي
   - جامعي
   - دراسات عليا
   - أخرى

4. هل قمت باستخدام تطبيق الدفع الالكتروني MTN Cash من قبل؟

- نعم
- لا

ملاحظة: تم استخدام مقياس ليكرت الخماسي بالأسئلة التالية:

المحور الأول: أمان التطبيق:

5. أشعر أن بياناتي تبقى خاصة وآمنة عند استخدام التطبيق.
6. التطبيق يرسل لي إشعاراً فورياً عند إجراء أي عملية دفع
7. أحياناً يطلب مني التطبيق رمز تحقق إضافي يصل إلى هاتفي قبل إتمام العملية.
8. أعتقد أن التطبيق لديه وسائل لحمايتي من محاولات الاحتيال.

المحور الثاني: الحملات التسويقية الأمنية

9. الإعلانات الخاصة بالتطبيق أشعرتني أن التطبيق آمن للاستخدام.
10. المعلومات التي يقدمها التطبيق عن الأمان ساعدتني على الثقة باستخدامه.
11. أوضح لي تسويق التطبيق أن الشركة تهتم بحماية أموالي وبياناتي.
12. الرسائل النصية أو الإشعارات من التطبيق جعلتني أشعر أن بياناتي محمية

المحور الثالث: تعقيد الإجراءات الأمنية

13. الدخول إلى التطبيق سهل وبسيط
14. أحياناً أشعر أن خطوات الأمان في التطبيق كثيرة وتستغرق وقتاً.
15. كثرة التحقق الأمني تجعل المعاملة أبطأ.
16. بعض الإجراءات الأمنية تجعل استخدام التطبيق أقل راحة.

المحور الرابع: ثقة العملاء

17. أشعر بالاطمئنان عند إجراء المدفوعات باستخدام التطبيق.
18. أثق أن التطبيق يحمي أموالي ومعلوماتي الشخصية.
19. لدي ثقة بأن الشركة المشغلة للتطبيق ملتزمة بتأمين بياناتي.
20. أرى أن التطبيق أكثر أماناً من الطرق التقليدية للدفع.

المحور الخامس: تبني التطبيق

21. أستخدم التطبيق بشكل متكرر لإجراء مدفوعاتي.
22. أنصح الآخرين باستخدام هذا التطبيق.
23. أنوي الاستمرار في استخدام التطبيق مستقبلاً.
24. أفضل هذا التطبيق على التطبيقات الأخرى المتوفرة.

ثانياً: مجموعات التركيز

المرحلة الأولى: الترحيب والتعارف

السؤال 1: التعريف والترحيب

"أرحب بالجميع هنا، نشكركم على قبولكم المشاركة في هذا النقاش. قبل أن نبدأ، هل يمكن لكل واحد منكم أن يقدم نفسه باختصار: اسمك (أو اللقب فقط إن أردت)، عملك، وكم سنة تستخدم تطبيقMTN Cash ؟"

المرحلة الثانية: أسئلة التمهيد والإحماء

السؤال 2: التجربة الأولى

"أخبرونا عن أول مرة استخدمتم فيها تطبيق MTN Cash كيف عرفتم عن التطبيق؟ ما الذي دفعكم لتجربته؟ وكيف كانت؟

المرحلة الثالثة: أسئلة الاستكشاف الرئيسية

المحور الأول: أمان التطبيق

السؤال 3: الشعور العام بالأمان

"عندما تستخدمون التطبيق لتحويل الأموال أو الدفع، ما الذي يجعلكم تشعرون بالأمان؟ وبالعكس، ما الذي قد يُقلقكم أو يُخيفكم؟"

السؤال 4: تجارب حقيقية مع الأمان

"هل حدثت معكم موقف شعرتم فيه أن التطبيق حماكم من خطر ما؟ أو موقف شعرتم فيها بالقلق على أمان أموالكم؟ شارك معنا إن أردت".

السؤال 5: ميزات الأمان المطلوبة

"نتحدث قليلاً عن ميزات الأمان الموجودة: رمز التحقق، البصمة، الإشعارات الفورية. هل هذه الميزات كافية من وجهة نظركم؟ ما الذي تتمنون إضافته؟"

المحور الثاني: الحملات التسويقية الأمنية

السؤال 6: الوعي بالحملات الإعلانية

"هل شاهدتم إعلانات أو حملات ترويجية لتطبيقMTN Cash ؟ في أي مكان شاهدتموها؟ ما الذي تتذكرونه عنها؟ وما انطباعكم؟"

السؤال 7: الرسالة التسويقية المفضلة

"عندما تشاهدون إعلاناً عن تطبيق دفع إلكتروني، ما الرسالة التي تجذب انتباهكم أكثر؟ هل هي: الأمان؟ السهولة والسرعة؟ العروض والخصومات؟ ثقة الشركة؟ شيء آخر؟"

السؤال 8: لو كنتم مسؤولي التسويق

"لو طُلب منكم تصميم إعلان لتطبيقMTN Cash ، ما الرسالة الأساسية التي ستركزون عليها؟ ومن الجمهور المستهدف حسب رأيكم؟ وعلى أي قنوات ستبثونه؟"

المحور الثالث: تعقيد الإجراءات الأمنية(Security Procedures Complexity)

السؤال 9: تقييم سهولة الاستخدام

"كيف تصفون تجربتكم العملية مع التطبيق؟ هل تجدون الدخول والخروج سهلاً؟ وكيف تشعرون تجاه خطوات الأمان مثل رمز التحقق والبصمة؟ هل هي سهلة أم معقدة؟"

السؤال 10: التخلي عن المعاملات بسبب التعقيد

"هل سبق أن توقفتم أو تخليتم عن إتمام معاملة بسبب كثرة الخطوات الأمنية أو استغراقها وقتاً؟ أخبرونا: كم مرة حدث هذا؟ وفي أي مواقف؟"

السؤال 11: التوازن المثالي

"تخيلوا معي هذا التوازن: بين الأمان والسرعة. هل تفضلون أماناً أكثر حتى لو كان أبطأ؟ أم سرعة أكثر مع أمان أقل؟ ما هو التوازن المثالي من وجهة نظركم؟"

المحور الرابع: ثقة العملاء

السؤال 12: مصادر الثقة

"ما الذي يجعلكم تثقون أو لا تثقون في تطبيق للدفع الإلكتروني بشكل عام؟ وكيف تقيّمون ثقتكم في MTN Cashتحديداً؟ ما أسباب ثقتكم أو عدم ثقتكم؟"

السؤال 13: التأثير الاجتماعي على الثقة

"هل ثقتكم في التطبيق تأثرت بشيء سمعتموه من الآخرين؟ قصص من صديق أو قريب استخدمه؟ أم قصص فشل أو احتيال؟ كيف أثرت هذه القصص على قرارك؟"

السؤال 14: المقارنة مع الطرق التقليدية

"لو قارنتم بين أمان التطبيق والطرق التقليدية مثل حمل النقود أو الذهاب للبنك أو استخدام البطاقات البنكية، ما رأيكم؟ أيهما أكثر أماناً؟ وأيهما أكثر موثوقية؟"

المحور الخامس: تبني التطبيق

السؤال 15: أنماط الاستخدام

"في أي المواقف تستخدمون التطبيق بشكل أساسي؟ هل تستخدمونه يومياً؟ أسبوعياً؟ لعمليات معينة فقط؟ وهل هناك مواقف تفضلون فيها طرق دفع أخرى؟ لماذا؟"

السؤال 16: التوصية والنية المستقبلية

"هل نصحتم أحداً باستخدام التطبيق؟ ماذا قلتم لهم؟ وهل هناك من نصحتموه بعدم استخدامه؟ لماذا؟ وهل تنوون الاستمرار في استخدام التطبيق مستقبلاً؟"

السؤال 17: عوامل التخلي عن الاستخدام

"ما الذي قد يجعلكم تتوقفون عن استخدام التطبيق؟ أي سيناريو أو مشكلة ستدفعكم للانتقال لبديل آخر؟ وبالعكس، ما الذي سيجعلكم تستخدمونه أكثر؟"

المرحلة الرابعة: أسئلة التعمق والتفصيل

السؤال 18: الاقتراحات الثلاثة الأولى

"لو كنتم مسؤولين عن تطوير التطبيق والشركة المشغلة، ما أول ثلاثة أشياء ستغيرونها أو تحسّنونها؟ رتّبوها حسب الأولوية: ما الأهم؟ ما الثاني؟ ما الثالث؟"

المرحلة الخامسة: الختام

السؤال 19: السؤال المفتوح النهائي

"قبل أن ننهي، هل هناك شيء لم نسأل عنه وتودون مشاركته معنا؟ أي ملاحظة أو اقتراح أو تعليق نسينا أن نغطيه؟"