

رسالة ماجستير بعنوان :

دور إدارة المخاطر الرقمية في تشغيل تطبيقات التوصيل واثرها تقنياً
(تطبيق جاهز نموذجاً)

إعداد الطالب/ة /

ريم هديب الجبني

إشراف/

د. الفیصل عبد الحمید

د. فايز جراد

العام الدراسي:

٢٠٢٤

Midocean University
College of Management
Department/specialization of
risk management



Master's Thesis:

**The Role of Digital Risk Management in Operating Delivery Applications and
Its Technical Impact**

(A Case Study of Jahez Application)

Prepared by:

Reem AL-johani

Supervised by:

Dr. Al-Faisal Abdel Hamid

Dr. Fayez Jarad

Academic Year: 2024

حقوق الطباعة

حقوق الطباعة لهذه الرسالة تملكها الجامعة .

ملخص الدراسة :

تعد إدارة المخاطر الرقمية من المجالات الحيوية في ظل التطور التكنولوجي المتسارع وزيادة الاعتماد على الأنظمة الرقمية في العمليات اليومية. تزداد التهديدات السيبرانية التي تستهدف البيانات الحساسة والأنظمة الرقمية، مما يجعل تبني استراتيجيات فعالة لإدارة هذه المخاطر أمراً ضرورياً لحماية الأصول الرقمية وضمان استمرارية الخدمات. تركز هذه الدراسة على تحليل دور إدارة المخاطر الرقمية في تشغيل تطبيقات التوصيل، مع التركيز على تطبيق "جاهز" كنموذج. يهدف البحث إلى فهم تأثير إدارة المخاطر الرقمية على كفاءة وأمان تشغيل تطبيقات التوصيل من الناحية التقنية، واستكشاف الحلول الممكنة لتحسين الأمن والكفاءة.

من خلال استخدام المنهج الوصفي التحليلي، تم جمع البيانات عبر المراجعة الأدبية، والاستبيانات، وتحليلها باستخدام الأساليب الإحصائية المناسبة. أظهرت النتائج أن غالبية المستخدمين يستخدمون التطبيق بشكل غير منتظم، إلا أنهم يعبرون عن رضاهم العالي عن سرعة التوصيل وجودة الخدمات المقدمة. كما أظهرت النتائج تفضيلاً كبيراً للدفع الإلكتروني عبر Apple Pay، وشعوراً عالياً بالأمان والثقة في إجراءات الأمان المتبعة في التطبيق. اعتبر معظم المستخدمين أن الإجراءات الأمنية فعالة أو مقبولة، مما يعزز الثقة في التطبيق وقدرته على حماية بياناتهم الشخصية.

تخلص الدراسة إلى أهمية تعزيز استراتيجيات إدارة المخاطر الرقمية لتحسين كفاءة وأمان تشغيل تطبيقات التوصيل. توصي الدراسة بتقديم برامج ولاء وعروض خاصة لتعزيز الاستخدام المتكرر، تحسين العمليات اللوجستية لتسريع التوصيل، وتوسيع خيارات الدفع لتلبية تفضيلات المستخدمين. كما توصي بتحسين إجراءات حماية البيانات وزيادة الوعي بأهمية الأمان الإلكتروني بين المستخدمين، والاستمرار في تقديم التحديثات والتحسينات الدورية لضمان التكيف مع تطلعات المستخدمين والتطورات التكنولوجية.

الكلمات المفتاحية :

إدارة المخاطر الرقمية - تطبيقات التوصيل - الأمان السيبراني - حماية البيانات - تطبيق "جاهز" - الكفاءة التشغيلية - تجربة المستخدم - الدفع الإلكتروني - تحديثات التطبيقات - التحليل الوصفي التحليلي

Abstract

Digital risk management is a critical area in the context of rapid technological advancement and increased reliance on digital systems in daily operations. The rise in cyber threats targeting sensitive data and digital systems necessitates the adoption of effective strategies to manage these risks and protect digital assets while ensuring service continuity. This study focuses on analyzing the role of digital risk management in the operation of delivery applications, using the "Jahez" application as a model. The research aims to understand how digital risk management impacts the technical efficiency and security of delivery applications and explore possible solutions to enhance security and efficiency.

Using a descriptive–analytical methodology, data was collected through literature review, and surveys, and analyzed using appropriate statistical methods. The results indicated that the majority of users use the application irregularly, but they express high satisfaction with the delivery speed and quality of services provided. The results also showed a strong preference for electronic payment through Apple Pay and a high sense of security and trust in the security measures implemented by the application. Most users considered the security measures effective or acceptable, enhancing confidence in the application's ability to protect their personal data.

The study concludes that it is essential to enhance digital risk management strategies to improve the efficiency and security of delivery applications. The study recommends introducing loyalty programs and special offers to encourage frequent use, improving logistical processes to speed up delivery, and expanding payment options to meet user preferences. It also recommends enhancing data protection measures, increasing awareness of the importance of cybersecurity among users, and continuously providing updates and improvements to ensure the application meets user expectations and technological developments.

Keywords:

Digital Risk Management – Delivery Applications – Cybersecurity – Data Protection – Jahez Application – Operational Efficiency – User Experience – Electronic Payment – Application Updates – Descriptive Analytical Analysis

الشكر والتقدير :

يسرني أن أتوجه بالشكر والتقدير الى :

– لعائلتي

– لكل من ساعدني على انجاز هذه الدراسة .

فهارس الموضوعات

الموضوع	رقم الصفحة
الفصل الأول : الاطار العام للدراسة	
المقدمة	١
مشكلة الدراسة	١
أهداف الدراسة + أسئلة الدراسة	٢
فرضيات الدراسة + أهمية الدراسة	٣
حدود الدراسة	٤
مصطلحات الدراسة	٥
الدراسات السابقة	٦
هيكل الدراسة (تقسيمها)	١٠
الفصل الثاني: الإطار النظري	
النظريات والمفاهيم العلمية المتعلقة بإدارة المخاطر الرقمية وتطبيقات التوصيل	
مفهوم إدارة المخاطر الرقمية	١٢
نظريات إدارة المخاطر التقليدية والحديثة	١٤
استراتيجيات إدارة المخاطر الرقمية	١٦
تطبيقات التوصيل: مفهومها وأهميتها	١٩
٥. تحليل المخاطر الرقمية في تطبيقات التوصيل	٢١
٦. إدارة المخاطر الرقمية في تطبيق "جاهز"	٢٣
٧. دراسة تطبيق "جاهز" كنموذج	٢٥
الفصل الثالث: منهجية الدراسة	
تمهيد	٢٧
التحليل البياني لإجابات محاور الاستبانة	٢٨
الفصل الرابع: النتائج والتوصيات	
النتائج + مناقشة النتائج	٣٨
التوصيات	٣٩
مناقشة التوصيات	٤٠
الخاتمة	٤١
المراجع	٤٣
الملاحق	٤٥

قائمة بالجداول

الجدول	رقم الصفحة
جدول (١-٢) يوضح أنواع المخاطر الرقمية وتأثيرها	١٣
جدول (٢-٢) مقارنة بين نظريات إدارة المخاطر التقليدية والحديثة	١٦
جدول (٣-٢) يوضح استراتيجيات الوقاية والحماية	١٩
جدول (٤-٢) يوضح أهمية تطبيقات التوصيل	٢١
جدول (٥-٢) يوضح تأثير المخاطر الرقمية	٢٢
جدول (٦-٢) أمثلة واقعية على المخاطر الرقمية وتأثيراتها	٢٣
جدول (٧-٢) يوضح استراتيجيات الأمان في "جاهز" وتحليل فعاليتها	٢٥
جدول (١-٣): جدول المتوسط والانحراف المعياري	٣٦
جدول (١-٤) : يوضح توزيع الإجابات على الأسئلة المختلفة	٤٧

قائمة بالأشكال

الشكل	رقم الصفحة
شكل (١-٢) : يوضح المخاطر الرقمية وتأثيراتها	١٣
شكل (٢-٢) : يوضح نموذج CIA (Confidentiality, Integrity, Availability):	١٦
شكل (٣-٢) يوضح استراتيجيات إدارة المخاطر	١٩
شكل (٤-٢) يوضح تحديات تطبيقات التوصيل التقنية	٢١
شكل (١-٣): معلومات العمر	٢٨
شكل (٢-٣): معلومات الجنس	٢٨
شكل (٣-٣): معلومات المنطقة الجغرافية	٢٩
شكل (٤-٣): يوضح عدد مرات استخدام تطبيق جاهز في الشهر	٢٩
شكل (٥-٣): يوضح مدى الرضا عن سرعة توصيل الطلبات	٣٠
شكل (٦-٣): يوضح طريقة الدفع المستخدمة	٣٠
شكل (٧-٣): هل البيانات امنة عند استخدام تطبيق جاهز	٣١
شكل (٨-٣): تقييم فعالية الإجراءات الأمنية في تطبيق جاهز	٣١
شكل (٩-٣): توضيح اي مشاكل امنييه واجهة المستخدم عند استخدام التطبيق	٣٢
شكل (١٠-٣): توضيح مدى رضا المستخدمين عن جودة الخدمات المقدمة من خلال التطبيق	٣٣
شكل (١١-٣): ملاحظة وجود تحديثات وتحسينات دورية في تطبيق جاهز	٣٣
شكل (١٢-٣): توضيح حول تلقى اشعارات كافية حول طلبك	٣٤
شكل (١٣-٣): توضيح حول توصي الاخرين باستخدام تطبيق جاهز	٣٥
شكل (١٤-٣): مخطط يوضح المتوسط والانحراف المعياري	٣٧

قائمة بالمصطلحات

المصطلح	تعريفه علمياً وإجرائياً
إدارة المخاطر الرقمية	- التعريف العلمي: هي عملية تحديد وتحليل وتقييم التهديدات الرقمية المحتملة ووضع استراتيجيات للحد من تأثيرها على الأنظمة الرقمية. (إبراهيم ، ٢٠٢٣) - التعريف الإجرائي: في هذه الدراسة، تشير إلى الإجراءات والسياسات المتبعة لحماية تطبيقات التوصيل من التهديدات السيبرانية وضمان استمرارية العمليات التشغيلية.
تطبيقات التوصيل	- التعريف العلمي: هي البرمجيات التي تستخدم تكنولوجيا المعلومات لتقديم خدمات توصيل المنتجات أو الطعام إلى العملاء. (أبن يوب وآخرون ، ٢٠٢٢) - التعريف الإجرائي: في هذه الدراسة، تشير إلى التطبيقات الرقمية مثل "جاهز" التي تسهل عملية توصيل الطلبات من المطاعم أو المتاجر إلى المستهلكين.
الأمن السيبراني	- التعريف العلمي: هو مجموعة من التقنيات والممارسات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات والاختراقات الإلكترونية. (إحليل ، ٢٠٢٤) - التعريف الإجرائي: في هذه الدراسة، تشير إلى التدابير الأمنية المتخذة لحماية البيانات والمعلومات في تطبيقات التوصيل من التهديدات الإلكترونية.
حماية البيانات	- التعريف العلمي: هي عملية تأمين البيانات من الوصول غير المصرح به أو التعديل أو التدمير. - التعريف الإجرائي: في هذه الدراسة، تشير إلى التدابير التقنية والتنظيمية المستخدمة لحماية بيانات العملاء والمعلومات الحساسة في تطبيقات التوصيل. (أبو عتيقة، ٢٠٢١)
التهديدات الإلكترونية	- التعريف العلمي: هي أي عمل خبيث يستهدف سرقة البيانات أو تعطيل العمليات أو إتلاف النظام الرقمي. (دحماني ، ٢٠٢٣) - التعريف الإجرائي: في هذه الدراسة، تشير إلى المخاطر المحتملة التي يمكن أن تؤثر على سلامة وأمان تطبيقات التوصيل.
تقنيات التشفير	- التعريف العلمي: هي عمليات رياضية تستخدم لتحويل البيانات إلى صيغة غير قابلة للقراءة إلا من قبل الأشخاص المصرح لهم (جراح ، ٢٠٠٩). - التعريف الإجرائي: في هذه الدراسة، تشير إلى الأساليب التقنية المستخدمة لحماية البيانات في تطبيقات التوصيل من الاختراق والوصول غير المصرح به.

• التعريف العلمي: هي فشل أو خلل في النظام التقني يؤدي إلى توقف الخدمة أو تأثير سلبي على الأداء. (علي ، ٢٠١٦) • التعريف الإجرائي: في هذه الدراسة، تشير إلى أي مشكلة تقنية تؤدي إلى تعطيل خدمة تطبيقات التوصيل وتؤثر تجربة المستخدم.	الأعطال التقنية
• التعريف العلمي: الذكاء الاصطناعي هو مجال من علوم الحاسوب يهدف إلى إنشاء أنظمة قادرة على أداء مهام تتطلب ذكاءً بشرياً. التعلم الآلي هو فرع من الذكاء الاصطناعي يتيح للنظام التعلم والتحسين من خلال التجربة. (أحرز الله ، ٢٠١٩) • التعريف الإجرائي : في هذه الدراسة، تشير إلى التقنيات المستخدمة في تحسين كفاءة وفعالية تشغيل تطبيقات التوصيل.	الذكاء الاصطناعي والتعلم الآلي
• التعريف العلمي: هي جميع الجوانب المتعلقة بتفاعل المستخدم النهائي مع الشركة وخدماتها ومنتجاتها. (مرسى ، ٢٠٢٣) • التعريف الإجرائي: في هذه الدراسة، تشير إلى رضا العملاء وسهولة استخدام تطبيقات التوصيل والتفاعل معها.	تجربة المستخدم
• التعريف العلمي: هو منصة رقمية تقدم خدمات توصيل الطعام من المطاعم إلى العملاء. (الغرباوي ، ٢٠٢٢) • التعريف الإجرائي: في هذه الدراسة، يُستخدم تطبيق "جاهز" كنموذج لتطبيقات التوصيل لدراسة كيفية إدارة المخاطر الرقمية وتحليل تأثيرها التقني.	تطبيق "جاهز"

الفصل الأول :

الاطار العام للدراسة

المقدمة :

في عصر التحول الرقمي السريع والتقدم التكنولوجي المتسارع، أصبحت إدارة المخاطر الرقمية جزءاً أساسياً من عملية تشغيل وتطوير التطبيقات الرقمية، ولا سيما تطبيقات التوصيل. تعتمد هذه التطبيقات بشكل كبير على التكنولوجيا في تنفيذ العمليات اليومية، مما يجعلها عرضة للعديد من المخاطر الرقمية التي قد تؤثر على كفاءتها وأمنها. تتضمن إدارة المخاطر الرقمية مجموعة من السياسات والإجراءات التي تهدف إلى حماية البيانات والمعلومات الرقمية من التهديدات الإلكترونية والاختراقات. تشمل هذه الإجراءات تقييم المخاطر المحتملة، تطوير استراتيجيات لتقليل هذه المخاطر، وتطبيق التقنيات اللازمة لضمان سلامة وأمان الأنظمة الرقمية.

تشهد تطبيقات التوصيل نمواً متسارعاً في جميع أنحاء العالم، حيث أصبحت جزءاً لا يتجزأ من الحياة اليومية للعديد من الأشخاص. تعتمد هذه التطبيقات على تقنيات متقدمة مثل الذكاء الاصطناعي، التعلم الآلي، ونظم المعلومات الجغرافية لتحسين خدماتها وتلبية احتياجات العملاء بكفاءة عالية. ومع ذلك، تعتمد تطبيقات التوصيل بشكل كبير على البنية التحتية الرقمية، مما يجعلها عرضة للعديد من المخاطر التقنية مثل الهجمات السيبرانية، اختراق البيانات، والأعطال التقنية التي قد تتسبب في توقف الخدمة وتأثر تجربة المستخدم.

تلعب إدارة المخاطر الرقمية دوراً محورياً في حماية تطبيقات التوصيل من هذه المخاطر. من خلال تطبيق استراتيجيات فعالة لإدارة المخاطر، يمكن تقليل احتمالية وقوع الحوادث الأمنية وتحسين الاستجابة في حال حدوثها. تشمل هذه الاستراتيجيات التقييم الدوري للأمن السيبراني، تطبيق تقنيات التشفير لحماية البيانات الحساسة، وتدريب الموظفين على أفضل الممارسات الأمنية لضمان الالتزام بالإجراءات الوقائية.

يعتبر تطبيق "جاهز" مثالاً عملياً لتطبيقات التوصيل الناجحة التي تولي اهتماماً كبيراً لإدارة المخاطر الرقمية. يعتمد جاهز على مجموعة من الاستراتيجيات المتقدمة لضمان سلامة البيانات وكفاءة التشغيل. من خلال دراسة تطبيق جاهز، يمكن تسليط الضوء على أفضل الممارسات والتحديات التي تواجه تطبيقات التوصيل في هذا المجال. تُعد إدارة المخاطر الرقمية ركيزة أساسية لضمان استمرارية وكفاءة تشغيل تطبيقات التوصيل، وتظل ضرورة ملحة في ظل التهديدات المتزايدة في الفضاء السيبراني.

مشكلة الدراسة :

في ظل التوسع الكبير في استخدام تطبيقات التوصيل، يواجه مشغلو هذه التطبيقات تحديات متزايدة في الحفاظ على أمن البيانات وضمان استمرارية الخدمات بكفاءة عالية. تعتبر إدارة المخاطر الرقمية جزءاً أساسياً من هذه العملية، حيث أن أي خلل أو ضعف في التدابير الأمنية يمكن أن يؤدي إلى تعرض البيانات للاختراق، وتأثر تجربة المستخدم، وحتى فقدان الثقة في الخدمة. يهدف تطبيق "جاهز"، كنموذج للدراسة، إلى تسليط الضوء على كيفية تأثير إدارة المخاطر

الرقمية على تشغيل تطبيقات التوصيل من الناحية التقنية، واستكشاف الحلول الممكنة لتحسين الأمن والكفاءة. تركز الدراسة على تحليل التحديات الأمنية التي تواجه تطبيقات التوصيل وكيفية مواجهتها باستخدام استراتيجيات فعالة لإدارة المخاطر، لضمان حماية البيانات وتحسين جودة الخدمة المقدمة للمستخدمين.

أهداف الدراسة

١. تحديد المخاطر الرقمية الرئيسية التي تواجه تطبيقات التوصيل وتقييم تأثيرها على كفاءة وأمان التشغيل.
٢. تحليل كيفية تأثير المخاطر الرقمية على الأداء التقني لتطبيقات التوصيل وتجربة المستخدم.
٣. تقديم استراتيجيات فعالة لإدارة المخاطر الرقمية في تطبيقات التوصيل، مع التركيز على تقنيات التشفير والتقييم الدوري للأمن السيبراني.
٤. تحليل تطبيق "جاهز" كنموذج لدراسة كيفية تطبيق استراتيجيات إدارة المخاطر الرقمية على أرض الواقع.
٥. تقييم الحلول التقنية المستخدمة في حماية البيانات وتحسين كفاءة التشغيل في تطبيقات التوصيل.
٦. تقديم توصيات لتعزيز الأمن السيبراني في تطبيقات التوصيل من خلال التدريب المستمر للموظفين وتطبيق أفضل الممارسات الأمنية.
٧. دراسة تأثير استراتيجيات إدارة المخاطر الرقمية على تحسين تجربة المستخدم وزيادة رضا العملاء.
٨. توفير توصيات عملية للشركات لوضع سياسات وإجراءات أفضل لإدارة المخاطر الرقمية.
٩. مساعدة تطبيقات التوصيل على تعزيز تنافسيتها في السوق من خلال تطبيق استراتيجيات فعالة لإدارة المخاطر الرقمية.
١٠. تشجيع بناء ثقافة أمنية قوية داخل المؤسسات من خلال الالتزام بالإجراءات الوقائية والتدريب المستمر.

أسئلة الدراسة :

١. ما هي المخاطر الرقمية الرئيسية التي تواجه تطبيقات التوصيل؟
٢. كيف تؤثر هذه المخاطر على كفاءة وأمان تشغيل تطبيقات التوصيل؟
٣. ما هي الاستراتيجيات الفعالة لإدارة المخاطر الرقمية في تطبيقات التوصيل؟
٤. كيف يمكن لتقنيات التشفير أن تحمي البيانات الحساسة في تطبيقات التوصيل؟
٥. ما هو الدور الذي تلعبه عمليات التقييم الدوري للأمن السيبراني في تقليل المخاطر الرقمية؟
٦. كيف يمكن للتدريب المستمر للموظفين على أفضل الممارسات الأمنية أن يساهم في تحسين إدارة المخاطر الرقمية؟
٧. كيف يواجه تطبيق "جاهز" المخاطر الرقمية وما هي الاستراتيجيات التي يتبعها لضمان حماية البيانات وكفاءة التشغيل؟
٨. ما هي التحديات التقنية الرئيسية التي تواجه تطبيق "جاهز" وكيف يتم التغلب عليها؟
٩. ما هو تأثير التحول الرقمي على إدارة المخاطر في تطبيقات التوصيل؟

١٠. كيف يمكن تحسين تجربة المستخدم من خلال تعزيز الأمن السيبراني في تطبيقات التوصيل؟

فرضيات الدراسة :

- ١) هناك علاقة سلبية بين عدم وجود استراتيجيات فعالة لإدارة المخاطر الرقمية وكفاءة تشغيل تطبيقات التوصيل.
- ٢) استخدام تقنيات التشفير يقلل بشكل كبير من احتمالية اختراق البيانات في تطبيقات التوصيل.
- ٣) التقييم الدوري للأمن السيبراني يساهم في تحديد نقاط الضعف ومعالجتها بفعالية في تطبيقات التوصيل.
- ٤) التدريب المستمر للموظفين على أفضل الممارسات الأمنية يعزز من قدرة تطبيقات التوصيل على مواجهة المخاطر الرقمية.
- ٥) تطبيق "جاهز" ينجح في تنفيذ استراتيجيات متقدمة لإدارة المخاطر الرقمية مما يؤدي إلى تحسين حماية البيانات وكفاءة التشغيل.
- ٦) تحديات التحول الرقمي تزيد من الحاجة إلى إدارة مخاطر رقمية فعالة لضمان استمرارية وكفاءة خدمات التوصيل.
- ٧) تعزيز الأمن السيبراني في تطبيقات التوصيل يؤدي إلى تحسين تجربة المستخدم وزيادة الثقة في الخدمة.
- ٨) استراتيجيات إدارة المخاطر الرقمية الفعالة تساهم في تقليل الأعطال التقنية في تطبيقات التوصيل.
- ٩) هناك علاقة إيجابية بين جودة استراتيجيات إدارة المخاطر الرقمية ورضا العملاء عن تطبيقات التوصيل.
- ١٠) تطبيقات التوصيل التي تعتمد على استراتيجيات متقدمة لإدارة المخاطر الرقمية تحقق أداءً أفضل في السوق مقارنةً بتلك التي لا تعتمد على مثل هذه الاستراتيجيات.

أهمية الدراسة :

الأهمية العلمية :

- تساهم الدراسة في توسيع الفهم النظري حول المخاطر الرقمية التي تواجه تطبيقات التوصيل، وتقديم رؤى علمية حول كيفية تحليلها وإدارتها.
- تساعد الدراسة في تطوير وتقييم استراتيجيات جديدة وفعالة لإدارة المخاطر الرقمية، مما يمكن أن يكون مرجعاً أكاديمياً للأبحاث المستقبلية.
- تساهم الدراسة في فهم تأثير التقنيات الحديثة مثل الذكاء الاصطناعي والتعلم الآلي على إدارة المخاطر الرقمية في تطبيقات التوصيل.
- توفر الدراسة قاعدة علمية تدعم الأبحاث التطبيقية والتجريبية في مجال الأمن السيبراني وتطبيقات التوصيل.

الأهمية العملية :

- من خلال تحديد المخاطر الرقمية وتقديم استراتيجيات فعالة لإدارتها، يمكن للتطبيقات تحسين كفاءتها وأمانها، مما يزيد من رضا العملاء وثقتهم.

- تقدم الدراسة تطبيق "جاهز" كنموذج عملي، مما يساعد الشركات الأخرى في فهم كيفية تطبيق استراتيجيات إدارة المخاطر الرقمية بفعالية.
- من خلال تحسين إدارة المخاطر الرقمية، يمكن تقليل الأعطال التقنية والاختراقات الأمنية، مما يقلل من الخسائر المالية المحتملة.
- توفر الدراسة توصيات عملية يمكن أن تساعد الشركات في وضع سياسات وإجراءات أفضل لإدارة المخاطر الرقمية.
- من خلال تطبيق أفضل الممارسات في إدارة المخاطر الرقمية، يمكن لتطبيقات التوصيل تعزيز تنافسيتها في السوق وتحقيق أداء أفضل.
- يساهم تحسين الأمن السيبراني في تعزيز تجربة المستخدم، مما يؤدي إلى زيادة الرضا والولاء للتطبيقات.
- تشجع الدراسة على بناء ثقافة أمنية قوية داخل المؤسسات من خلال التدريب المستمر والالتزام بأفضل الممارسات الأمنية.

حدود الدراسة :

الحدود المكانية :

- تقتصر الدراسة على تطبيقات التوصيل في المملكة العربية السعودية، مع التركيز على تطبيق "جاهز" كنموذج لدراسة المخاطر الرقمية واستراتيجيات إدارتها.

الحدود الزمانية :

- تغطي الدراسة الفترة الزمنية من يوليو ٢٠٢٤ إلى ديسمبر ٢٠٢٤، وذلك لتحليل البيانات والنتائج المتعلقة بإدارة المخاطر الرقمية خلال هذه الفترة.

الحدود الموضوعية :

- تركز الدراسة على تحليل المخاطر الرقمية التي تواجه تطبيقات التوصيل واستراتيجيات إدارتها، دون التطرق إلى جوانب أخرى مثل الجوانب اللوجستية أو التسويقية لتطبيقات التوصيل.

الحدود البشرية :

- تشمل الدراسة تحليلاً للممارسات والسياسات المتبعة من قبل العاملين في تطبيق "جاهز" والمسؤولين عن إدارة المخاطر الرقمية، بالإضافة إلى جمع آراء وتجارب المستخدمين النهائيين لتطبيق "جاهز".

الحدود المنهجية :

- تعتمد الدراسة على المنهج الوصفي التحليلي لتحليل البيانات والمعلومات المتعلقة بإدارة المخاطر الرقمية في تطبيقات التوصيل، مع التركيز على دراسة حالة تطبيق "جاهز".

تعريف مصطلحات الدراسة :

■ إدارة المخاطر الرقمية :

- **التعريف العلمي :** هي عملية تحديد وتحليل وتقييم التهديدات الرقمية المحتملة ووضع استراتيجيات للحد من تأثيرها على الأنظمة الرقمية. (إبراهيم ، ٢٠٢٣)
- **التعريف الإجرائي :** في هذه الدراسة، تشير إلى الإجراءات والسياسات المتبعة لحماية تطبيقات التوصيل من التهديدات السيبرانية وضمان استمرارية العمليات التشغيلية.

■ تطبيقات التوصيل :

- **التعريف العلمي :** هي البرمجيات التي تستخدم تكنولوجيا المعلومات لتقديم خدمات توصيل المنتجات أو الطعام إلى العملاء. (ابن يوب وآخرون ، ٢٠٢٢)
- **التعريف الإجرائي :** في هذه الدراسة، تشير إلى التطبيقات الرقمية مثل "جاهز" التي تسهل عملية توصيل الطلبات من المطاعم أو المتاجر إلى المستهلكين.

■ الأمن السيبراني :

- **التعريف العلمي :** هو مجموعة من التقنيات والممارسات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات والاختراقات الإلكترونية. (إحليل ، ٢٠٢٤)
- **التعريف الإجرائي :** في هذه الدراسة، تشير إلى التدابير الأمنية المتخذة لحماية البيانات والمعلومات في تطبيقات التوصيل من التهديدات الإلكترونية.

■ حماية البيانات :

- **التعريف العلمي :** هي عملية تأمين البيانات من الوصول غير المصرح به أو التعديل أو التدمير.
- **التعريف الإجرائي :** في هذه الدراسة، تشير إلى التدابير التقنية والتنظيمية المستخدمة لحماية بيانات العملاء والمعلومات الحساسة في تطبيقات التوصيل. (أبو عتيقة، ٢٠٢١)

■ التهديدات الإلكترونية :

- **التعريف العلمي :** هي أي عمل خبيث يستهدف سرقة البيانات أو تعطيل العمليات أو إتلاف النظام الرقمي. (دحماني ، ٢٠٢٣)
- **التعريف الإجرائي :** في هذه الدراسة، تشير إلى المخاطر المحتملة التي يمكن أن تؤثر على سلامة وأمان تطبيقات التوصيل.

■ تقنيات التشفير :

- **التعريف العلمي :** هي عمليات رياضية تستخدم لتحويل البيانات إلى صيغة غير قابلة للقراءة إلا من قبل الأشخاص المصرح لهم (جراح ، ٢٠٠٩).
- **التعريف الإجرائي :** في هذه الدراسة، تشير إلى الأساليب التقنية المستخدمة لحماية البيانات في تطبيقات التوصيل من الاختراق والوصول غير المصرح به.

■ الأعطال التقنية :

- **التعريف العلمي:** هي فشل أو خلل في النظام التقني يؤدي إلى توقف الخدمة أو تأثير سلبي على الأداء. (علي ، ٢٠١٦)
- **التعريف الإجرائي:** في هذه الدراسة، تشير إلى أي مشكلة تقنية تؤدي إلى تعطيل خدمة تطبيقات التوصيل وتؤثر تجربة المستخدم.

■ الذكاء الاصطناعي والتعلم الآلي :

- **التعريف العلمي:** الذكاء الاصطناعي هو مجال من علوم الحاسوب يهدف إلى إنشاء أنظمة قادرة على أداء مهام تتطلب ذكاءً بشرياً. التعلم الآلي هو فرع من الذكاء الاصطناعي يتيح للنظام التعلم والتحسين من خلال التجربة. (أحرز الله ، ٢٠١٩)
- **التعريف الإجرائي :** في هذه الدراسة، تشير إلى التقنيات المستخدمة في تحسين كفاءة وفعالية تشغيل تطبيقات التوصيل.

■ تجربة المستخدم :

- **التعريف العلمي:** هي جميع الجوانب المتعلقة بتفاعل المستخدم النهائي مع الشركة وخدماتها ومنتجاتها. (مرسي ، ٢٠٢٣)
 - **التعريف الإجرائي:** في هذه الدراسة، تشير إلى رضا العملاء وسهولة استخدام تطبيقات التوصيل والتفاعل معها.
- ## ■ تطبيق "جاهز" :

- **التعريف العلمي:** هو منصة رقمية تقدم خدمات توصيل الطعام من المطاعم إلى العملاء. (الغرباوي ، ٢٠٢٢)
- **التعريف الإجرائي:** في هذه الدراسة، يُستخدم تطبيق "جاهز" كنموذج لتطبيقات التوصيل لدراسة كيفية إدارة المخاطر الرقمية وتحليل تأثيرها التقني.

الدراسات السابقة :

- دراسة النحاس ودبا (٢٠٢٢)، بعنوان "إدارة التحول الرقمي" هدفت دراسة رقمية لتقدير أهم التحولات الهيكلية التي تواجه المنظمات، والتعرف على آلية متنوعة ومتنوعة. حيث اشتركت في الاستخلاص الحديث إلى أن استخدام طبقات المجتمع والمتمثلة في التقنيات التحولية أصبح عاملاً أساسياً رقمياً للكومات والمنظمات والأعمال، لتأثيره المباشر في تطوير الأداء وإدارة جودة العمليات، بالإضافة إلى توفيره للموارد من وقت وجهد ومال فهو محرك أساسي للنمو في مكافحة الأمراض التي تنتهجها الرقمية، ورغم العديد من الجهود التي حققتها أهدافها باستخدام تقنيات التحول الرقمي إلا أن هناك مجموعة للتحول الرقمي قد تعيق تحقيق الامتداد المستمر في البقاء والنمو والتطور في بيئة الأعمال، بما في ذلك ما يتطلبه الاهتمام بهذه النظرية المتعددة على الرغم من استبعادها عن باقي الحالات التي تسمح لها بذلك تحديد طرق وسياسات تمويل هذه الخسارة، واستهداف الهدف الحالي الذي يمثل أهم أهداف التحول الرقمي الذي يواجه منظمات الأعمال، والتعرف على هذه الابتكارات المبتكرة.

- دراسة العتيبي (٢٠٢٣)، بعنوان "العمل في منصات النقل التشاركي: الفرص والتحديات: دراسة وصفية تحليلية من قطاع العمل في تطبيقات النقل والمركبات وتوصيل الطعام" هدفت الدراسة إلى تحليل العمل في لوحات النقل التشاركي الفرص والتحديات من عمل العاملين في تطبيقات النقل والأجرة وتوصيل الطعام. حيث يوضح الرسم إطاراً مفاهيمياً أوضح من خلاله مفهوم قواعد العمل التشاركي، والعاملين. كما بدأت في التكوين الوصفي للتحليل والكمي، وضبطت بيانات البيانات من استعادةها ٣٠٥ عامل. وتوصلت الدراسة إلى أن أهم الفرص المتاحة للإصدارات الحديثة هي ساعات عمل مرنة ثم توفير مالي مناسب وتوفير حل مؤقت. كما اختتمت الدراسة بتوصيات منها توفير قراءة من التسهيلات المتعلقة بموديلات السيارة.
- دراسة محمد (٢٠٢٠)، بعنوان "بناء تطبيق أندرويد لطلب بالتطبيق على مطعم سمكنا" هدفت الدراسة إلى بناء تطبيق مجاني لتعلم الإبداع طلب الدعم منها ويساهم في زيادة الإضافة للمطعم. حيث تم استخدام التطبيق الوصفي التحليلي في تحليل النظام عن طريق استخدام لغة العرف الموحد (UML) لغات البرمجة تصميم مواقع الويب في طريقة تصميم وبرمجة النظام واستخدام برنامج (Android Studio) في برمجة التطبيق. وتوصلت إلى الدراسة إلى أن التطبيق ساهم في تسهيل عملية الطلب من خلال الموبايل وتقليل الزمن والجهد على الزبون. ومن أهم النصائح هي بناء تطبيق أندرويد خاص بمدير النظام يمكن من إدارة التطبيق من خلال الموبايل بدلات من موقع الويب.
- دراسة العموش (٢٠٢١)، بعنوان "أثر توصيل الطعام على الأداء التسويقي للمطاعم في الأردن: دراسة حالة لتطبيق تأثير مايسترو في مدينة المفرق"، هدفت الدراسة إلى التعرف على تطبيقات توصيل الطعام (مايسترو) على أداء تسويق المطاعم في الأردن وتحديداً في مدينة المفرق ، والتعرف على مستوى الخدمة الميدانية من تطبيق توصيل الطعام عبر الإنترنت (مايسترو)، والتعرف على مستوى الأداء التسويقي للمطاعم التي تعمل ضمن تطبيق توصيل الطعام عبر الإنترنت (مايسترو)، والتعرف على وجود مساهم في توصيل الطعام عبر الإنترنت (مايسترو) على الأداء التسويقي للمطاعم التي تعمل على ذلك التطبيق. حيث تم استخدام النموذج الكمي الطبيعي لتطوير التطبيقات المتميزة على التقنية العالية، كما تم استخدام البرنامج الإحصائي (SPSS) وكرونباخ وفولفو التوزيع والتحليل العملي الاستكشافي. وخلصت الدراسة إلى أن مستوى الخدمة المقدمة من تطبيق مايسترو مرتفع للغاية بالإضافة إلى مستوى الأداء التسويقي للمطاعم العاملة من خلاله، وأوصت بالحفاظ على هذا المستوى المتقدم والصريح.
- دراسة العموش (٢٠٢١)، بعنوان "أثر توصيل الطعام على الأداء التسويقي للمطاعم في الأردن: دراسة حالة لتطبيق مايسترو في مدينة المفرق" هدفت الدراسة إلى التعرف على تطبيقات توصيل الطعام (مايسترو) على أداء تسويق المطاعم في الأردن وتحديداً في مدينة المفرق، والتعرف على مستوى الخدمة المقدمة من تطبيق توصيل الطعام عبر الإنترنت (مايسترو)، وكذلك الهدف المحدد على مستوى الأداء التسويقي للمطاعم التي تعمل ضمن تطبيق توصيل الطعام عبر الإنترنت (مايسترو)، والتعرف على وجود مساعد لتطبيق توصيل الطعام عبر الإنترنت (مايسترو) على الأداء التسويقي للمطاعم التي تعمل على ذلك التطبيق. تم استخدام الأمثلة الكميائية المطورة بفاصلها المميزة على التقنية العالية، كما تم استخدام البرنامج الإحصائي SPSS وكرونباخ

فولفو والتوزيع الطبيعي والتحليل العملي الاستكشافي. وخلصت الدراسة إلى أن مستوى الخدمة المقدمة من تطبيق مايسترو المرتفعات بالإضافة إلى مستوى الأداء التسويقي للمطاعم العاملة من خلاله، ووصت بالحفاظ على هذا المستوى المتقدم وأمنه.

(أوجه الشبه - الاختلاف - الاستفادة) بين هذه الدراسة والدراسات السابقة

■ أولاً : أوجه الشبه :

١. التقنيات التحولية واستخدام التكنولوجيا:

- دراسة النحاس ودبا : (2022) تناولت دور التحول الرقمي في تحسين الأداء والجودة في المنظمات، وأشارت إلى أهمية استخدام التكنولوجيا الحديثة في العمليات.
- دراسة محمد : (2020) تناولت بناء تطبيق أندرويد لتسهيل عمليات الطلب في المطاعم، واستخدمت تقنيات التحليل والتصميم الرقمي لتحسين الأداء.

٢. الفرص والتحديات في التطبيقات الرقمية:

- دراسة العتيبي : (2023) تناولت الفرص والتحديات في العمل على منصات النقل التشاركي، وأشارت إلى مرونة ساعات العمل والفرص المالية.
- الدراسة الحالية : تتناول إدارة المخاطر الرقمية في تشغيل تطبيقات التوصيل، مما يتضمن تحديات تقنية وأمنية مشابهة.

٣. الأثر على الأداء التسويقي والخدمات:

- دراسة العموش : (2021) تناولت أثر توصيل الطعام على الأداء التسويقي للمطاعم عبر تطبيق مايسترو.
- الدراسة الحالية : تدرس تأثير إدارة المخاطر الرقمية على تشغيل تطبيقات التوصيل وأدائها الفني والتقني.

■ ثانياً : أوجه الاختلاف :

١. نطاق الدراسة:

- دراسة النحاس ودبا : (2022) ركزت على التحول الرقمي بشكل عام وتأثيره على المنظمات.
- الدراسة الحالية : تركز بشكل خاص على إدارة المخاطر الرقمية في تطبيقات التوصيل (مثل تطبيق جاهز).

٢. المجال المحدد للتطبيق:

- دراسة محمد : (2020) ركزت على بناء تطبيق أندرويد لمطعم معين.
- الدراسة الحالية : تدرس تطبيقات التوصيل بشكل عام وليس تطبيقاً محدداً.

٣. الجوانب التقنية:

- دراسة العتيبي: (2023) تناولت الجوانب الاجتماعية والاقتصادية للعمل في تطبيقات النقل والتوصيل.
- الدراسة الحالية: تركز على الجوانب التقنية والأمنية لإدارة المخاطر في تشغيل تطبيقات التوصيل.

٤. المنهجية:

- دراسة العموش: (2021) استخدمت المنهج الكمي لتقييم الأداء التسويقي لتطبيق معين.
- الدراسة الحالية: تركز على تحليل المخاطر التقنية والأمنية، والتي قد تشمل استخدام مناهج تحليلية مختلفة.

كل الدراسات تشير إلى أهمية استخدام التكنولوجيا الحديثة وتحليل البيانات لتحسين الأداء وإدارة المخاطر، سواء كان ذلك في السياق التنظيمي العام أو في تطبيقات التوصيل والنقل التشاركي

■ ثالثاً : أوجه الاستفادة :

١. إطار نظري ومفاهيمي:

- دراسة النحاس ودبا (2022) تقدم إطاراً نظرياً حول أهمية التحول الرقمي في تحسين الأداء والجودة، مما يمكن الاستفادة منه في بناء إطار نظري مشابه للدراسة الحالية حول إدارة المخاطر الرقمية في تطبيقات التوصيل.

٢. تحليل التحديات التقنية والأمنية:

- دراسة العتيبي (2023) تقدم تحليلاً شاملاً للفرص والتحديات في العمل على منصات النقل التشاركي، مما يمكن استخدامه لتحديد التحديات التقنية والأمنية التي تواجه تطبيقات التوصيل مثل جاهز.

٣. استخدام التكنولوجيا لتحسين الأداء:

- دراسة محمد (2020) توضح كيفية استخدام التكنولوجيا لتحسين العمليات في المطاعم، مما يمكن أن يقدم أمثلة عملية لتحسين تطبيقات التوصيل من خلال الحلول التقنية المبتكرة.

٤. تقييم الأداء التسويقي:

- دراسة العموش (2021) تقدم منهجية لتقييم تأثير تطبيقات التوصيل على الأداء التسويقي، مما يمكن استخدامه لتقييم تأثير إدارة المخاطر الرقمية على أداء تطبيقات التوصيل.

٥. المنهجية البحثية:

- يمكن الاستفادة من المنهجيات المختلفة المستخدمة في الدراسات السابقة، مثل المنهج الكمي والتحليل الوصفي، لتصميم منهجية بحثية قوية ومتكاملة في الدراسة الحالية.

٦. التوصيات والسياسات:

- التوصيات التي قدمتها الدراسات السابقة بشأن تحسين الأداء وإدارة المخاطر يمكن أن تكون دليلاً لتقديم توصيات عملية وإجرائية لتطبيقات التوصيل في الدراسة الحالية.

كيفية التطبيق:

- تحليل البيانات :استخدام أساليب تحليل البيانات المستخدمة في الدراسات السابقة لتحليل بيانات تطبيق جاهز وتقييم فعالية إدارة المخاطر الرقمية.
 - دراسات الحالة :تطبيق النموذج التحليلي من دراسة العموش لتقييم تطبيق جاهز وتحليل الأداء التسويقي.
 - إطار العمل النظري :بناء إطار نظري يعتمد على نتائج دراسة النحاس ودبا لتحديد العوامل الأساسية لإدارة المخاطر الرقمية وتأثيرها على الأداء.
 - التحديات والحلول :الاستفادة من دراسة العتيبي لتحديد التحديات التقنية والأمنية في تطبيقات التوصيل واقتراح حلول مناسبة.
- بهذا الشكل، يمكن للدراسة الحالية أن تكون مدعومة بشكل جيد بالدراسات السابقة، مما يعزز من مصداقيتها ويسهم في تقديم نتائج وتوصيات أكثر فعالية ودقة

هيكل الدراسة (تقسيمها)

الفصل الأول: المقدمة

- مقدمة عامة :تقديم لموضوع الدراسة وأهميته في سياق التحول الرقمي وتطبيقات التوصيل.
- مشكلة الدراسة :تحديد المشكلة التي تتناولها الدراسة وأسباب اختيارها.
- أهداف الدراسة :عرض الأهداف التي تسعى الدراسة إلى تحقيقها.
- أسئلة الدراسة :تحديد الأسئلة التي تحاول الدراسة الإجابة عنها.
- فرضيات الدراسة :عرض الفرضيات التي سيتم اختبارها خلال الدراسة.
- أهمية الدراسة :بيان الأهمية العلمية والعملية للدراسة.
- حدود الدراسة :تحديد الحدود المكانية والزمانية والموضوعية والمنهجية للدراسة.
- مصطلحات الدراسة :تعريف المصطلحات والمفاهيم الأساسية المستخدمة في الدراسة.

الفصل الثاني: الإطار النظري

- الإطار النظري :عرض النظريات والمفاهيم العلمية المتعلقة بإدارة المخاطر الرقمية وتطبيقات التوصيل.

الفصل الثالث: منهجية الدراسة

- المنهجية :توضيح المنهج الوصفي التحليلي المستخدم في الدراسة.
- أدوات جمع البيانات :شرح الأدوات والأساليب المستخدمة لجمع البيانات (المراجعة الأدبية، المقابلات، الاستبيانات).
- مجتمع وعينة الدراسة :وصف المجتمع المستهدف وعينة الدراسة.
- طرق تحليل البيانات :شرح الأساليب الإحصائية والتحليلية المستخدمة لتحليل البيانات.

الفصل الرابع: مناقشة النتائج والتوصيات

- تحليل البيانات :عرض وتحليل البيانات التي تم جمعها من خلال أدوات جمع البيانات.
- النتائج :تقديم النتائج الرئيسية التي تم التوصل إليها بناءً على تحليل البيانات.
- مناقشة النتائج :تفسير ومناقشة النتائج في ضوء الأدبيات السابقة والفرضيات.
- الخاتمة :تلخيص لأهم ما توصلت إليه الدراسة، مع اقتراحات لأبحاث مستقبلية.
- المراجع :قائمة بالمراجع العلمية والأدبية التي تم الاستعانة بها في إعداد الدراسة.

الفصل الثاني: الإطار النظري

النظريات والمفاهيم العلمية المتعلقة بإدارة المخاطر الرقمية وتطبيقات التوصيل

١. مفهوم إدارة المخاطر الرقمية

▪ تعريف وأهمية إدارة المخاطر الرقمية :

تعريف إدارة المخاطر الرقمية:

إدارة المخاطر الرقمية هي عملية منهجية تهدف إلى تحديد وتقييم والتحكم في التهديدات التي يمكن أن تؤثر على الأصول الرقمية للمؤسسة، بما في ذلك البيانات، الأنظمة، الشبكات، والتطبيقات. يتضمن ذلك تحليل مخاطر الهجمات الإلكترونية، الفيروسات، البرامج الخبيثة، والاختراقات الأمنية، ووضع سياسات وإجراءات للتعامل معها بفعالية.

▪ أهمية إدارة المخاطر الرقمية:

- حماية البيانات: تضمن إدارة المخاطر الرقمية حماية البيانات الحساسة والمعلومات الشخصية من الاختراقات والسرقات.
- ضمان استمرارية الأعمال: من خلال وضع خطط للتعامل مع الطوارئ، تساهم إدارة المخاطر الرقمية في الحفاظ على استمرارية العمليات الحيوية للمؤسسة.
- تحقيق الامتثال: تساعد على الامتثال للمعايير والقوانين المتعلقة بأمن المعلومات وحماية البيانات.
- تعزيز الثقة: تعزيز الثقة بين العملاء والشركاء التجاريين من خلال توفير بيئة آمنة ومعتمدة.
- تقليل التكاليف: تقليل التكاليف المحتملة المرتبطة بالاختراقات الأمنية وتعطل الأنظمة.

▪ أنواع المخاطر الرقمية

يمكن تصنيف المخاطر الرقمية إلى عدة أنواع، تشمل:

١. المخاطر السيبرانية:

- الهجمات الإلكترونية: تشمل الهجمات التي تهدف إلى تعطيل الأنظمة أو سرقة البيانات، مثل هجمات DDoS والبرامج الضارة.

- الاختراقات: محاولات غير مصرح بها للوصول إلى الأنظمة والمعلومات.

٢. المخاطر التقنية:

- أعطال النظام: فشل الأجهزة أو البرمجيات الذي يؤدي إلى توقف العمليات.
- نقاط الضعف في البرمجيات: وجود ثغرات في البرمجيات يمكن استغلالها من قبل المهاجمين.

٣. المخاطر البشرية:

- الأخطاء البشرية: الأخطاء التي يرتكبها الموظفون والتي قد تؤدي إلى تسريب البيانات أو تعطيل الأنظمة.

○ الهندسة الاجتماعية :استخدام الخداع للحصول على معلومات حساسة من المستخدمين.

٤. المخاطر التشغيلية:

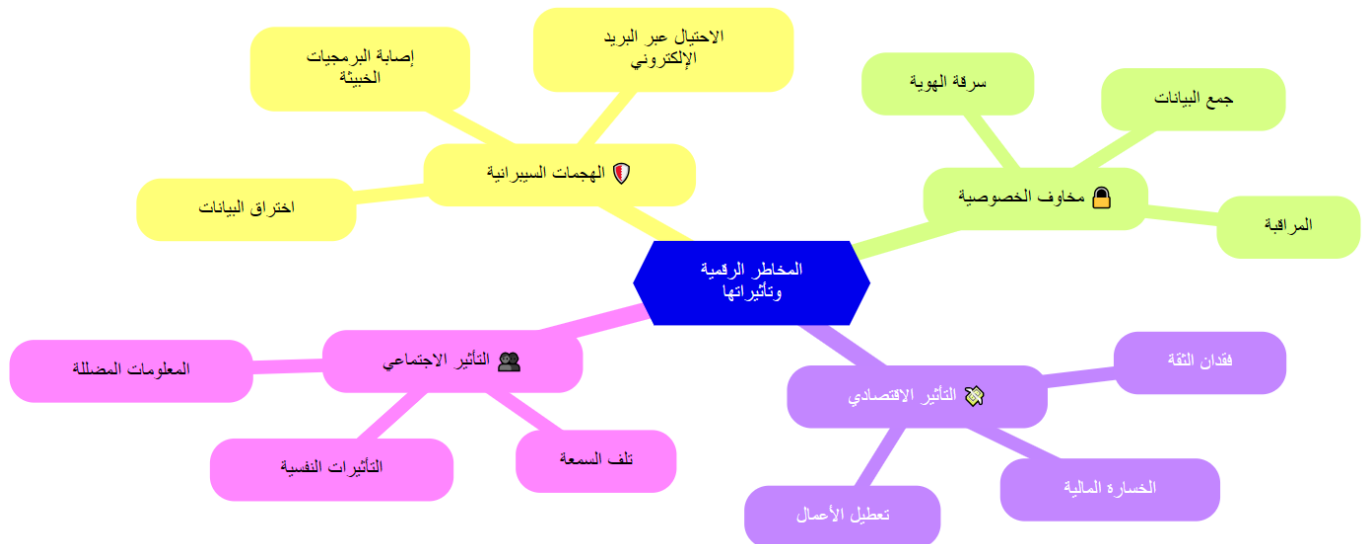
- فقدان البيانات :فقدان البيانات الهامة نتيجة لأخطاء بشرية أو أعطال تقنية.
- عدم كفاية التدابير الأمنية :نقص الإجراءات الأمنية اللازمة لحماية الأصول الرقمية.

٥. المخاطر البيئية:

- الكوارث الطبيعية :تأثير الزلازل، الفيضانات، والحرائق على البنية التحتية الرقمية.
- الانقطاع الكهربائي :تأثير انقطاع الكهرباء على تشغيل الأنظمة الرقمية.

جدول (٢-١) يوضح أنواع المخاطر الرقمية وتأثيرها

النوع	أمثلة	التأثير
المخاطر السيبرانية	هجمات DDoS ، الفيروسات، الاختراقات	تعطل الأنظمة، سرقة البيانات
المخاطر التقنية	أعطال الأجهزة، ثغرات البرمجيات	توقف العمليات، استغلال الثغرات
المخاطر البشرية	أخطاء الموظفين، الهندسة الاجتماعية	تسريب البيانات، وصول غير مصرح به
المخاطر التشغيلية	فقدان البيانات، نقص التدابير الأمنية	فقدان المعلومات، ضعف الحماية الأمنية
المخاطر البيئية	الزلازل، الفيضانات، الانقطاع الكهربائي	تلف البنية التحتية، توقف الأنظمة



شكل (٢-١) : يوضح المخاطر الرقمية وتأثيراتها

٢. نظريات إدارة المخاطر التقليدية والحديثة :

أولاً : نظريات إدارة المخاطر التقليدية :

١. نظرية إدارة المخاطر التقليدية:

- التعريف :تُعنى بتحديد وتقييم المخاطر التي قد تواجه المؤسسة ووضع استراتيجيات لتجنبها أو تقليل تأثيرها.
- الخطوات:

- التعرف على المخاطر :تحديد جميع المخاطر المحتملة التي يمكن أن تواجه المؤسسة.
- تحليل المخاطر :تقييم احتمالية حدوث كل مخاطرة وتأثيرها المحتمل.
- التحكم في المخاطر :تطوير وتنفيذ استراتيجيات للتحكم في المخاطر وتخفيف تأثيرها.
- مراقبة المخاطر :متابعة وتقييم فعالية استراتيجيات إدارة المخاطر وتعديلها حسب الحاجة.

٢. نظرية إدارة المخاطر الشاملة:(Enterprise Risk Management – ERM)

- التعريف :تركز على إدارة المخاطر في جميع أقسام المؤسسة بطريقة متكاملة لضمان تحقيق أهداف المؤسسة.
- المكونات:

- تحديد السياق :فهم البيئة الداخلية والخارجية للمؤسسة.
- تقييم المخاطر :تحليل تأثير المخاطر على أهداف المؤسسة.
- تطوير استراتيجيات إدارة المخاطر :تصميم استراتيجيات شاملة للتحكم في المخاطر.
- مراقبة ومراجعة :متابعة وتقييم استراتيجيات إدارة المخاطر وتحديثها بانتظام.

ثانياً : نظريات إدارة المخاطر الحديثة :

١. نظرية إدارة المخاطر السيبرانية:

- التعريف :تركز على تحديد وتحليل وإدارة المخاطر المرتبطة بالنظم الرقمية والبيئة السيبرانية.
- الخطوات:

- تقييم المخاطر السيبرانية :تحليل التهديدات السيبرانية ونقاط الضعف في النظم الرقمية.
- تطوير استراتيجيات الحماية :تصميم وتنفيذ سياسات وإجراءات لحماية الأصول الرقمية.
- التصدي للهجمات :وضع خطط للتصدي للهجمات السيبرانية عند حدوثها.
- التعافي :تطوير خطط لاستعادة الأنظمة والخدمات بعد الهجمات.

٢. نظرية الدفاع في العمق:(Defense in Depth)

- التعريف :تعتمد على استخدام طبقات متعددة من الدفاع لحماية الأصول الرقمية من الهجمات.

○ المكونات:

- الحماية المادية: تأمين الوصول إلى الأجهزة والمعدات.
- الحماية الفنية: استخدام تقنيات مثل جدران الحماية وأنظمة الكشف عن التسلل.
- الحماية التنظيمية: وضع سياسات وإجراءات أمنية وتدريب الموظفين.

▪ نظريات الأمن السيبراني :

١. نموذج: (CIA (Confidentiality, Integrity, Availability

- التعريف: إطار عمل أساسي في مجال الأمن السيبراني يركز على ثلاث نقاط رئيسية:
- السرية: (Confidentiality) حماية المعلومات من الوصول غير المصرح به.
- السلامة: (Integrity) ضمان دقة واكتمال المعلومات.
- التوافر: (Availability) ضمان توفر المعلومات والأنظمة للمستخدمين المصرح لهم عند الحاجة.

○ التطبيقات:

- تشفير البيانات: لضمان سرية المعلومات.
- التحكم في الوصول: لضمان أن فقط المستخدمين المصرح لهم يمكنهم الوصول إلى المعلومات.
- التكرار والنسخ الاحتياطي: لضمان توفر المعلومات والأنظمة.

٢. نظرية الدفاع في العمق: (Defense in Depth)

- التعريف: استراتيجية أمنية تعتمد على استخدام طبقات متعددة من الدفاع لضمان الحماية الشاملة.
- المكونات:

- الحماية المادية: تأمين المعدات والأجهزة.
- الحماية التقنية: استخدام جدران الحماية وأنظمة الكشف عن التسلل.
- الحماية الإدارية: وضع سياسات أمنية وتدريب الموظفين.

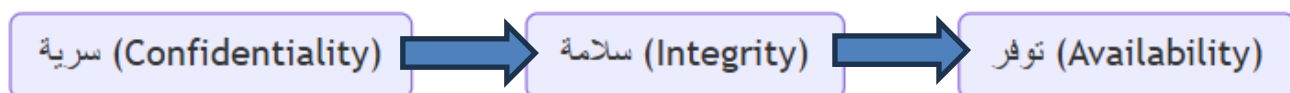
○ التطبيقات:

- جدران الحماية: لمنع الوصول غير المصرح به.
- أنظمة كشف التسلل: لمراقبة واكتشاف الأنشطة غير العادية.
- سياسات الأمن: لتوجيه سلوك الموظفين وضمان التزامهم بالإجراءات الأمنية.

٣. نموذج NIST للأمن السيبراني:

- التعريف: إطار شامل لإدارة المخاطر السيبرانية يشمل خمسة مجالات رئيسية:
- التعرف: (Identify) تحديد الأصول المهمة ونقاط الضعف.
- الحماية: (Protect) تطوير وتنفيذ تدابير الحماية.
- الكشف: (Detect) مراقبة الأنظمة لاكتشاف الأنشطة غير العادية.

- الاستجابة: (Respond) وضع خطط للاستجابة للحوادث الأمنية.
- الاستعادة: (Recover) تطوير خطط لاستعادة الأنظمة والخدمات بعد الحوادث.
- التطبيقات:
- تقييم المخاطر: تحديد وتقييم نقاط الضعف والتهديدات.
- تطوير السياسات: وضع سياسات وإجراءات لحماية الأصول الرقمية.
- التدريب: تدريب الموظفين على أفضل الممارسات الأمنية.



شكل (٢-٢) : يوضح نموذج CIA (Confidentiality, Integrity, Availability)

جدول (٢-٢) مقارنة بين نظريات إدارة المخاطر التقليدية والحديثة

المعيار	نظريات إدارة المخاطر التقليدية	نظريات إدارة المخاطر الحديثة
التركيز	الوقاية والتحكم في المخاطر	التعامل مع التهديدات الرقمية المتطورة
الأدوات المستخدمة	تحليل المخاطر، خطط الطوارئ	الذكاء الاصطناعي، التعلم الآلي
النطاق	جميع أنواع المخاطر	المخاطر السيبرانية والتقنية
الأمثلة	إدارة المخاطر الشاملة (ERM)	نظرية إدارة المخاطر السيبرانية

٣. استراتيجيات إدارة المخاطر الرقمية :

▪ الوقاية والحماية

الوقاية والحماية:

الوقاية والحماية هي الخطوات الأولية في استراتيجية إدارة المخاطر الرقمية وتهدف إلى منع حدوث المخاطر أو تقليل احتمالية حدوثها. تشمل هذه الاستراتيجيات العديد من الإجراءات والتقنيات المصممة لضمان سلامة وأمان الأصول الرقمية.

الإجراءات الوقائية:

١. جدران الحماية: (Firewalls)

- تعريف: جدار الحماية هو نظام أمني يراقب ويضبط حركة المرور الواردة والصادرة استنادًا إلى قواعد الأمان المحددة.

- الفائدة: حماية الشبكة من الهجمات الخارجية والحفاظ على البيانات الحساسة.

٢. برامج مكافحة الفيروسات: (Antivirus Software)

- تعريف: برنامج مصمم للكشف عن الفيروسات وإزالتها من الأجهزة.
- الفائدة: حماية الأجهزة من البرمجيات الضارة والهجمات الفيروسية.

٣. أنظمة كشف التسلل: (Intrusion Detection Systems – IDS)

- تعريف: أنظمة مصممة للكشف عن الأنشطة غير العادية أو المشبوهة داخل الشبكة.
- الفائدة: تنبيه المسؤولين عن الأمن إلى الأنشطة غير المصرح بها قبل أن تتحول إلى هجمات ضارة.

٤. تحديث البرمجيات: (Software Updates)

- تعريف: عملية تثبيت التحديثات والباتشات الجديدة للبرمجيات والتطبيقات.
- الفائدة: إصلاح الثغرات الأمنية وتحسين أداء البرمجيات.

٥. التحقق الثنائي: (Two-Factor Authentication – 2FA)

- تعريف: نظام أمني يتطلب من المستخدمين تقديم شكلين من أشكال التحقق قبل الوصول إلى النظام.
- الفائدة: تعزيز أمان الحسابات والتأكد من هوية المستخدمين.

■ الكشف والتصدي :

الكشف والتصدي هما خطوات متقدمة في استراتيجية إدارة المخاطر الرقمية وتركز على اكتشاف الأنشطة الضارة بسرعة والتصدي لها بفعالية. تشمل هذه الاستراتيجيات تقنيات وأدوات لمراقبة الأنظمة واكتشاف أي سلوك غير طبيعي.

الكشف:

١. مراقبة الشبكة: (Network Monitoring)

- تعريف: عملية مراقبة حركة المرور على الشبكة لاكتشاف الأنشطة غير العادية.
- الفائدة: التعرف على التهديدات المحتملة واستجابة فورية.

٢. أنظمة كشف التسلل: (Intrusion Detection Systems – IDS)

- تعريف: أنظمة تراقب الأنشطة داخل الشبكة وتحدد الأنشطة غير المصرح بها.
- الفائدة: توفير تنبيهات فورية للمسؤولين عن الأمن.

٣. تحليل السجلات: (Log Analysis)

- تعريف: تحليل سجلات النظام لتحديد الأنشطة غير العادية.
- الفائدة: اكتشاف الأنشطة المشبوهة وتحديد مصدرها.

التصدي:

١. إجراءات الاستجابة للحوادث: (Incident Response Procedures)

- تعريف: مجموعة من الإجراءات المتبعة للتعامل مع الحوادث الأمنية عند حدوثها.
- الفائدة: تقليل تأثير الحوادث الأمنية وتسريع عملية التعافي.

٢. التصدي التلقائي: (Automated Response Systems)

- تعريف: أنظمة تلقائية تتخذ إجراءات محددة عند اكتشاف تهديد معين.
- الفائدة: سرعة التصدي للتهديدات وتقليل الأضرار.

٣. العزل: (Isolation)

- تعريف: فصل الأنظمة المصابة عن الشبكة لمنع انتشار الهجوم.
- الفائدة: حماية بقية الشبكة من التأثير بالهجوم.

■ التعافي والاستجابة

تعريف التعافي والاستجابة:

التعافي والاستجابة هي المراحل النهائية في استراتيجية إدارة المخاطر الرقمية وتهدف إلى إعادة الأنظمة إلى حالتها الطبيعية بعد التعرض لحادث أمني وضمان استمرارية الأعمال.

التعافي:

١. استعادة البيانات: (Data Recovery)

- تعريف: عملية استعادة البيانات المفقودة أو المتضررة من النسخ الاحتياطية.
- الفائدة: تقليل فقدان البيانات وضمان استمرارية الأعمال.

٢. إعادة تهيئة الأنظمة: (System Re-imaging)

- تعريف: إعادة تثبيت الأنظمة والبرمجيات لإزالة أي برمجيات ضارة.
- الفائدة: ضمان سلامة النظام بعد الهجوم.

٣. اختبارات التعافي: (Recovery Testing)

- تعريف: اختبارات تهدف إلى التأكد من فعالية خطط التعافي واستعادة النظام.
- الفائدة: ضمان جاهزية الأنظمة للتعافي السريع في حالة الحوادث.

الاستجابة:

١. خطط الاستجابة للحوادث: (Incident Response Plans)

- تعريف: خطط مفصلة تحدد كيفية التعامل مع الحوادث الأمنية.
- الفائدة: توجيه الفريق الأمني في كيفية التصرف بسرعة وفعالية.

٢. التدريب والتوعية: (Training and Awareness)

- تعريف: برامج تدريبية لزيادة وعي الموظفين بكيفية التصرف عند وقوع حادث أمني.
- الفائدة: تقليل الأخطاء البشرية وزيادة كفاءة الاستجابة للحوادث.

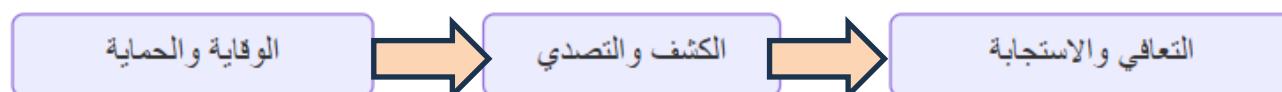
٣. تحليل ما بعد الحوادث: (Post-Incident Analysis)

- تعريف: تحليل شامل للحدث الأمني لتحديد أسبابه وطرق الوقاية منه في المستقبل.
- الفائدة: تحسين الإجراءات الأمنية وتقليل احتمال تكرار الحوادث.

جدول (٣-٢) يوضح استراتيجيات الوقاية والحماية

الإجراءات الوقائية	التعريف	الفائدة
جدران الحماية	نظام يراقب ويضبط حركة المرور الواردة والصادرة	حماية الشبكة من الهجمات الخارجية
برامج مكافحة الفيروسات	برنامج للكشف عن الفيروسات وإزالتها	حماية الأجهزة من البرمجيات الضارة
أنظمة كشف التسلل	أنظمة للكشف عن الأنشطة غير العادية	تنبيه المسؤولين عن الأنشطة غير المصرح بها
تحديث البرمجيات	تنصيب التحديثات والبثبات الجديدة	إصلاح الثغرات الأمنية
التحقق الثنائي	نظام يتطلب تقديم شكلين من التحقق	تعزيز أمان الحسابات

شكل (٣-٢) يوضح استراتيجيات إدارة المخاطر



٤. تطبيقات التوصيل: مفهومها وأهميتها

▪ تعريف وأهمية تطبيقات التوصيل :

تعريف تطبيقات التوصيل:

تطبيقات التوصيل هي برمجيات رقمية تُستخدم لتسهيل عملية نقل المنتجات أو الخدمات من المورد إلى المستهلك باستخدام التكنولوجيا. تعمل هذه التطبيقات على ربط العملاء بالموردين، مثل المطاعم أو المتاجر، وتتيح لهم طلب المنتجات أو الخدمات من خلال الهواتف الذكية أو الأجهزة الأخرى.

أهمية تطبيقات التوصيل:

١. راحة المستخدمين:

- الوصول السريع: تمكّن المستخدمين من طلب المنتجات أو الخدمات بسهولة وفي أي وقت ومن أي مكان.

- توفير الوقت والجهد: تقلل من حاجة المستهلكين لزيارة المتاجر أو المطاعم بأنفسهم.

٢. دعم الاقتصاد المحلي:

- زيادة المبيعات: تساعد المتاجر والمطاعم على الوصول إلى شريحة أوسع من العملاء وزيادة مبيعاتها.

○ خلق فرص عمل :تساهم في خلق فرص عمل جديدة للسائقين والعاملين في مجال التوصيل.

٣. تحسين تجربة العملاء :

○ التخصيص :توفر خيارات متعددة للمستخدمين من حيث المنتجات وطرق الدفع ووقت التوصيل.

○ التفاعل والتغذية الراجعة :تتيح للمستخدمين تقديم تقييمات وملاحظات حول الخدمات، مما يساعد على تحسين الجودة.

٤. تحسين الكفاءة التشغيلية:

○ إدارة الطلبات :تُمكّن الشركات من إدارة طلبات العملاء بكفاءة عالية.

○ تتبع الشحنات :توفر القدرة على تتبع الطلبات في الوقت الحقيقي، مما يعزز الشفافية والثقة.

■ التحديات التقنية :

■ التحديات التقنية التي تواجه تطبيقات التوصيل:

١. الأمن السيبراني:

○ التهديدات السيبرانية :تعرض التطبيقات للهجمات الإلكترونية التي يمكن أن تؤدي إلى اختراق البيانات وسرقة المعلومات الحساسة.

○ حماية البيانات :التحدي في تأمين بيانات المستخدمين والحفاظ على خصوصيتهم.

٢. استقرار الأنظمة والأداء:

○ الأعطال التقنية :مواجهة الأعطال والخلل في النظام يمكن أن يؤثر سلبًا على تجربة المستخدم ويؤدي إلى فقدان الطلبات.

○ تحمل الضغط :التحدي في ضمان استقرار النظام وأدائه عند زيادة عدد المستخدمين والطلبات.

٣. التكامل مع الأنظمة الأخرى:

○ التكامل التقني :صعوبة التكامل مع أنظمة الدفع الإلكتروني، نظم إدارة المخزون، وأنظمة التتبع.

○ التحديثات المستمرة :التحدي في مواكبة التحديثات التكنولوجية وإجراء التحديثات الدورية للتطبيقات.

٤. إدارة البيانات الكبيرة:

○ تحليل البيانات :الحاجة إلى تحليل كميات كبيرة من البيانات لاتخاذ قرارات مستنيرة حول تحسين الخدمة.

○ تخزين البيانات :التحدي في إدارة وتخزين البيانات بشكل فعال وآمن.

٥. التجربة المستخدمة:

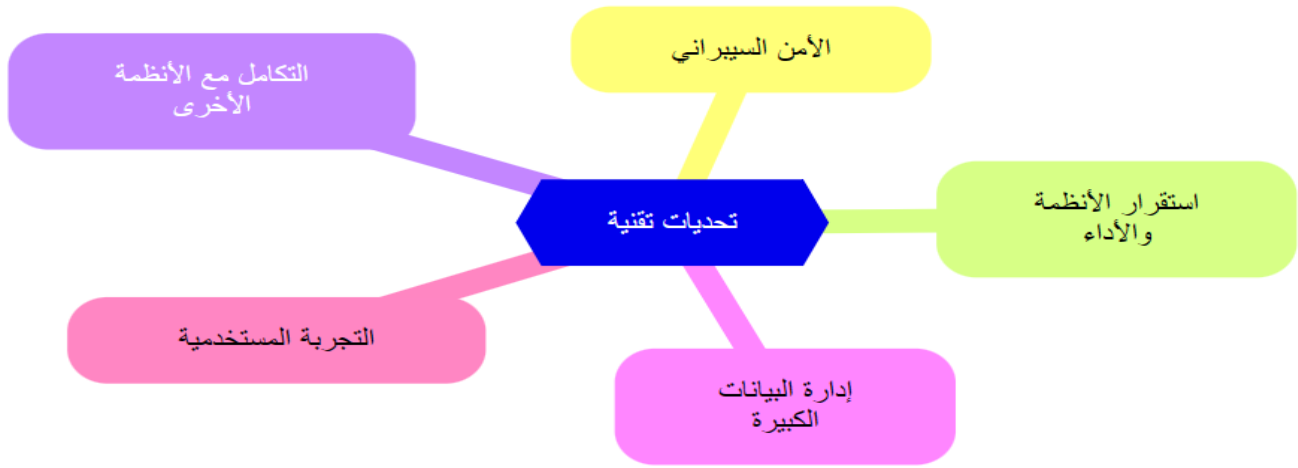
○ واجهة المستخدم :ضرورة تطوير واجهات مستخدم سهلة الاستخدام وفعالة لضمان تجربة سلسة.

○ دعم العملاء :التحدي في تقديم دعم فني مستمر وفعال للمستخدمين.

جدول (٢-٤) يوضح أهمية تطبيقات التوصيل

الأهمية	الشرح
راحة المستخدمين	تمكّن المستخدمين من طلب المنتجات بسهولة ومن أي مكان
دعم الاقتصاد المحلي	تساعد في زيادة مبيعات المتاجر والمطاعم وخلق فرص عمل
تحسين تجربة العملاء	توفر خيارات متعددة وتتيح التفاعل والتغذية الراجعة
تحسين الكفاءة التشغيلية	تمكن من إدارة الطلبات بكفاءة وتوفير تتبع الشحنات

شكل (٢-٤) يوضح تحديات تطبيقات التوصيل التقنية



٥. تحليل المخاطر الرقمية في تطبيقات التوصيل

■ أنواع وتأثير المخاطر الرقمية

أنواع المخاطر الرقمية في تطبيقات التوصيل:

١. الهجمات السيبرانية:

- تعريف: محاولات متعمدة لاختراق أنظمة التطبيقات وسرقة المعلومات أو تعطيل الخدمات.
- أمثلة: هجمات DDoS، الفيروسات، والبرامج الضارة.
- التأثير: توقف الخدمات، فقدان البيانات، وتأثر سمعة التطبيق.

٢. اختراق البيانات:

- تعريف: الوصول غير المصرح به إلى بيانات المستخدمين والشركة.
- أمثلة: سرقة معلومات الدفع، البيانات الشخصية، وسجلات الطلبات.
- التأثير: فقدان الثقة من قبل العملاء، تعويضات مالية، ومسائل قانونية.

٣. الأخطاء البشرية:

- تعريف: أخطاء الموظفين التي قد تؤدي إلى تسريب المعلومات أو تعرض النظام للاختراق.
- أمثلة: إرسال بيانات حساسة بالخطأ، استخدام كلمات مرور ضعيفة، والنقر على روابط ضارة.
- التأثير: تسريب البيانات، اختراق الأنظمة، وتعطل العمليات.

٤. نقاط الضعف في البرمجيات:

- تعريف: وجود ثغرات في البرمجيات يمكن أن يستغلها المهاجمون.
- أمثلة: ثغرات في نظام التشغيل، تطبيقات الويب، وبرمجيات الطرف الثالث.
- التأثير: إمكانية تنفيذ هجمات، تعطل الخدمات، وسرقة البيانات.

٥. التعرض للبرمجيات الخبيثة:

- تعريف: البرمجيات التي تصمم لإلحاق الضرر بالنظم الرقمية أو سرقة المعلومات.
- أمثلة: برامج الفدية (Ransomware)، وأحصنة طروادة (Trojans).
- التأثير: تشفير البيانات وطلب فدية، فقدان المعلومات، وتعطل الأنظمة.

٦. التهديدات الداخلية:

- تعريف: التهديدات التي تأتي من داخل المؤسسة، من الموظفين أو الأطراف ذات الصلة.
- أمثلة: سرقة بيانات الشركة، تسريب معلومات حساسة، وتخريب الأنظمة.
- التأثير: فقدان البيانات، الأضرار المالية، وتراجع الثقة.

جدول (٢-٥) يوضح تأثير المخاطر الرقمية

النوع	التأثير المحتمل
الهجمات السيبرانية	توقف الخدمات، فقدان البيانات، تأثر سمعة التطبيق
اختراق البيانات	فقدان الثقة، تعويضات مالية، مسائل قانونية
الأخطاء البشرية	تسريب البيانات، اختراق الأنظمة، تعطل العمليات
نقاط الضعف في البرمجيات	تنفيذ هجمات، تعطل الخدمات، سرقة البيانات
البرمجيات الخبيثة	تشفير البيانات وطلب فدية، فقدان المعلومات، تعطل الأنظمة
التهديدات الداخلية	فقدان البيانات، الأضرار المالية، تراجع الثقة

■ أمثلة واقعية

١. الهجوم على تطبيق "DoorDash"

- الحادثة: في ٢٠١٩، تعرضت DoorDash لهجوم سيبراني أدى إلى اختراق بيانات حوالي ٤.٩ مليون مستخدم.

- **التأثير:** سرقة معلومات شخصية ومعلومات الدفع، مما أثر على ثقة العملاء وأدى إلى تكبد الشركة تكاليف إضافية لتعزيز الأمان السيبراني.

٢. اختراق بيانات: "Zomato"

- **الحادثة:** في ٢٠١٧، تعرضت Zomato لاختراق أدى إلى تسريب بيانات حوالي ١٧ مليون مستخدم.
- **التأثير:** تم بيع البيانات على شبكة الإنترنت المظلمة، مما أدى إلى فقدان الثقة من قبل العملاء واضطرت الشركة إلى تحسين إجراءات الأمان.

٣. هجوم برمجيات الفدية على: "Just Eat"

- **الحادثة:** في ٢٠٢٠، تعرضت Just Eat لهجوم ببرمجيات الفدية أدى إلى تشفير بيانات الشركة وطلب فدية لإعادتها.
- **التأثير:** تعطل الخدمة لعدة ساعات، خسائر مالية مباشرة، وضرورة تحسين إجراءات الأمان لتجنب مثل هذه الهجمات مستقبلاً.

٤. الأخطاء البشرية في: "Uber Eats"

- **الحادثة:** في ٢٠١٩، أدى خطأ بشري إلى تسريب بيانات حساسة للعملاء عن طريق البريد الإلكتروني.
- **التأثير:** تعرض العملاء للخطر، وتكبدت الشركة تكاليف قانونية وتعويضات، بالإضافة إلى الحاجة لتدريب الموظفين على أفضل الممارسات الأمنية.

جدول (٢-٦) أمثلة واقعية على المخاطر الرقمية وتأثيراتها

التطبيق	الحادثة	التأثير
DoorDash	اختراق بيانات المستخدمين	سرقة معلومات شخصية ومعلومات الدفع، فقدان الثقة
Zomato	تسريب بيانات المستخدمين	بيع البيانات على الإنترنت المظلمة، تعزيز إجراءات الأمان
Just Eat	هجوم برمجيات الفدية	تشفير البيانات، خسائر مالية، تحسين الأمان
Uber Eats	تسريب بيانات عبر البريد الإلكتروني	تعرض العملاء للخطر، تكاليف قانونية، تدريب الموظفين

٦. إدارة المخاطر الرقمية في تطبيق "جاهز"

■ استراتيجيات الأمان وتحليل الفعالية

استراتيجيات الأمان في تطبيق "جاهز":

١. تشفير البيانات: (Data Encryption)

- **التعريف:** استخدام تقنيات التشفير لحماية البيانات أثناء النقل والتخزين.
- **التطبيق:** تطبيق "جاهز" يستخدم بروتوكولات تشفير متقدمة مثل (TLS) لضمان حماية بيانات المستخدمين ومعلومات الدفع.

٢. التحقق الثنائي: (Two-Factor Authentication – 2FA)

- **التعريف:** استخدام طبقتين من التحقق لتعزيز أمان الحسابات.
- **التطبيق:** يطلب "جهاز" من المستخدمين إدخال رمز تحقق يتم إرساله إلى هواتفهم المحمولة بالإضافة إلى كلمة المرور.

٣. جدران الحماية: (Firewalls)

- **التعريف:** نظام يراقب ويضبط حركة المرور بين الشبكات الموثوقة وغير الموثوقة.
- **التطبيق:** يقوم "جهاز" بتطبيق جدران حماية قوية لحماية البنية التحتية من الهجمات الخارجية.

٤. أنظمة كشف التسلل: (Intrusion Detection Systems – IDS)

- **التعريف:** أنظمة تراقب الأنشطة في الشبكة وتكتشف الأنشطة المشبوهة.
- **التطبيق:** يستخدم "جهاز" IDS للكشف المبكر عن أي محاولات تسلل أو أنشطة غير طبيعية.

٥. التحديثات الأمنية المنتظمة: (Regular Security Updates)

- **التعريف:** تحديث الأنظمة والتطبيقات بانتظام لسد الثغرات الأمنية.
- **التطبيق:** يقوم فريق الأمان في "جهاز" بإجراء تحديثات دورية لأنظمة التطبيق لضمان الحماية من الثغرات الأمنية الجديدة.

■ تحليل الفعالية

تحليل فعالية استراتيجيات الأمان:

١. مراقبة وتحليل الحوادث: (Incident Monitoring and Analysis)

- **التحليل:** يتم تحليل جميع الحوادث الأمنية لتحديد أسبابها وكيفية منعها في المستقبل.
- **النتائج:** يساعد هذا التحليل في تحسين استراتيجيات الأمان وتعزيز فعالية التدابير الأمنية.

٢. اختبارات الاختراق: (Penetration Testing)

- **التعريف:** إجراء اختبارات لاختراق الأنظمة بواسطة مختصين لاكتشاف الثغرات.
- **التطبيق:** يجري "جهاز" اختبارات اختراق دورية لتقييم مدى أمان النظام واكتشاف نقاط الضعف.

٣. التدريب والتوعية: (Training and Awareness)

- **التعريف:** تدريب الموظفين على أفضل الممارسات الأمنية وكيفية التعامل مع الحوادث.
- **التطبيق:** يوفر "جهاز" دورات تدريبية منتظمة للموظفين حول الأمان السيبراني وكيفية التصرف في حالات الطوارئ.

٤. تقييم الأمان الدوري: (Periodic Security Audits)

- **التعريف:** إجراء مراجعات دورية لنظم الأمان للتحقق من فعاليتها.
- **التطبيق:** يجري "جهاز" تقييمات أمان دورية لتحديد نقاط الضعف والتحسينات المطلوبة.

٧. دراسة تطبيق "جاهز" كنموذج

دراسة حالة: تطبيق "جاهز":

١. الوصف العام:

- **التعريف:** "جاهز" هو تطبيق توصيل رائد في المملكة العربية السعودية، يتيح للمستخدمين طلب الطعام والمنتجات من المطاعم والمتاجر القريبة.
- **الهدف:** توفير خدمة توصيل سريعة وآمنة للمستخدمين مع التركيز على حماية بياناتهم وسلامة المعاملات.

٢. استراتيجيات الأمان المطبقة:

- **التشفير:** يستخدم "جاهز" تقنيات التشفير لحماية البيانات أثناء النقل والتخزين.
- **التحقق الثنائي:** يتم استخدام التحقق الثنائي لحماية حسابات المستخدمين.
- **جدران الحماية وأنظمة كشف التسلل:** لحماية البنية التحتية من الهجمات الخارجية والأنشطة غير الطبيعية.
- **التحديثات الأمنية المنتظمة:** لضمان سد الثغرات الأمنية والحماية من التهديدات الجديدة.

٣. فعالية استراتيجيات الأمان:

- **تقليل الحوادث الأمنية:** أدى تطبيق استراتيجيات الأمان إلى تقليل عدد الحوادث الأمنية والتسريبات.
- **تحسين ثقة المستخدمين:** ساهمت إجراءات الأمان القوية في زيادة ثقة المستخدمين واستمرار استخدامهم للتطبيق.
- **الاستجابة السريعة للحوادث:** بفضل التدريب والتوعية، يتمكن فريق "جاهز" من الاستجابة السريعة للحوادث الأمنية وتقليل تأثيرها.

٤. التحديات والحلول:

- **التحديات:** مثل التهديدات السيبرانية المتطورة والاحتياجات المستمرة للتحديثات الأمنية.
- **الحلول:** تشمل الاستثمار في تقنيات أمان جديدة، تحسين البنية التحتية الأمنية، وتقديم تدريب مستمر للموظفين.

جدول (٧-٢) يوضح استراتيجيات الأمان في "جاهز" وتحليل فعاليتها

الاستراتيجية	الوصف	الفعالية
تشفير البيانات	حماية البيانات أثناء النقل والتخزين	تقليل مخاطر تسريب البيانات
التحقق الثنائي	إضافة طبقة أمان إضافية للحسابات	تعزيز أمان الحسابات وتقليل الاختراقات
جدران الحماية وأنظمة كشف التسلل	حماية البنية التحتية من الهجمات	تقليل عدد الحوادث الأمنية والهجمات
التحديثات الأمنية المنتظمة	سد الثغرات الأمنية بانتظام	حماية من التهديدات الجديدة وزيادة الأمان

يتناول الإطار النظري للدراسة إدارة المخاطر الرقمية في تطبيقات التوصيل مع التركيز على تطبيق "جاهز" كنموذج، حيث تشمل إدارة المخاطر الرقمية تحديد وتحليل والتحكم في التهديدات التي تواجه الأصول الرقمية لضمان حماية البيانات واستمرارية الأعمال. تتضمن نظريات إدارة المخاطر التقليدية مثل إدارة المخاطر الشاملة (ERM) والحديثة مثل إدارة المخاطر السيبرانية، بالإضافة إلى نظريات الأمن السيبراني كنموذج CIA ونظرية الدفاع في العمق. تشمل استراتيجيات إدارة المخاطر الرقمية الوقاية والحماية باستخدام جدران الحماية وبرامج مكافحة الفيروسات، الكشف والتصدي من خلال مراقبة الشبكة وأنظمة كشف التسلل، والتعافي والاستجابة باستعادة البيانات وإعادة تهيئة الأنظمة. تبرز أهمية تطبيقات التوصيل في تحسين كفاءة العمليات وتعزيز تجربة المستخدم، مع التحديات التقنية مثل الأمن السيبراني واستقرار الأنظمة. يشمل تحليل المخاطر الرقمية في تطبيقات التوصيل أنواع المخاطر وتأثيراتها مثل الهجمات السيبرانية واختراق البيانات، مع أمثلة واقعية من تطبيقات مثل DoorDash و Zomato. يوضح تحليل تطبيق "جاهز" استراتيجيات الأمان المطبقة وفعاليتها في تقليل الحوادث الأمنية وتحسين ثقة المستخدمين.

الفصل الثالث: منهجية الدراسة

• تمهيد

يتضمن هذا الفصل وصفا للطريقة والإجراءات التي اتبعتها الباحثة في تحديد مجتمع الدراسة وعينتها، واستخدام أداة الدراسة، وخطوات التحقق من صدق الأداة وثباتها، إضافة إلى وصف تصميم الدراسة والطرق الإحصائية المتبعة في تحليل البيانات.

• منهج الدراسة:

تهدف هذه الدراسة إلى تحليل دور إدارة المخاطر الرقمية في تشغيل تطبيقات التوصيل، باستخدام تطبيق "جاهز" كنموذج. لتحقيق هذا الهدف، تم اعتماد منهجية بحثية تجمع بين الأساليب الكمية والنوعية لجمع وتحليل البيانات.

• مجتمع الدراسة

يتكون مجتمع الدراسة من جميع مستخدمي تطبيق "جاهز" في المملكة العربية السعودية. يشمل هذا المجتمع مجموعة متنوعة من الأفراد الذين يستخدمون التطبيق لأغراض التوصيل المختلفة.

• عينة الدراسة

تم اختيار عينة عشوائية تتألف من ٩٣ شخص من مستخدمي تطبيق "جاهز" في المملكة. تم تحديد هذه العينة بناءً على معايير معينة لضمان تنوع المشاركين وشمولهم لمختلف الفئات العمرية.

• أداة الدراسة:

استخدمت الدراسة الاستبيان كأداة رئيسية لجمع البيانات. تم تصميم الاستبيان بعناية ليتضمن مجموعة من الأسئلة التي تغطي الجوانب المختلفة لإدارة المخاطر الرقمية في تطبيق "جاهز".

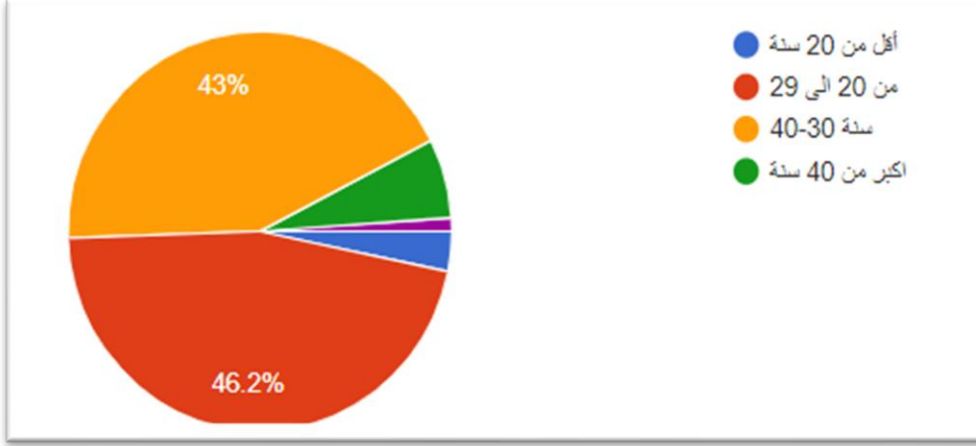
• جمع البيانات

تم توزيع الاستبيان على عينة الدراسة عبر وسائل التواصل الإلكتروني لضمان الوصول إلى أكبر عدد ممكن من المشاركين. تم جمع البيانات خلال فترة زمنية محددة لضمان الحصول على معلومات دقيقة ومحدثة.

التحليل البياني

أولاً: المعلومات الديموغرافية

■ العمر



شكل (٣-١): معلومات العمر

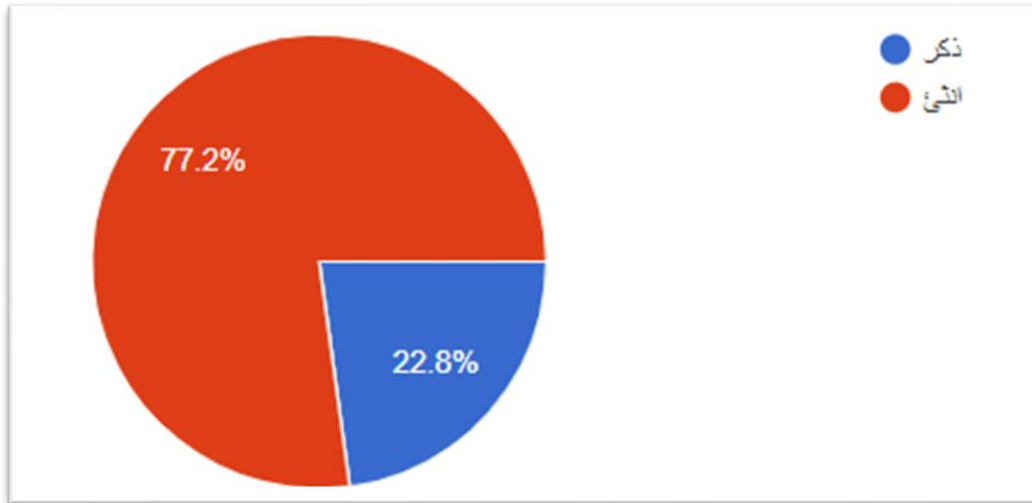
الفئة العمرية من ٢٠ إلى ٢٩ سنة تشكل النسبة الأكبر بواقع ٤٦.٢٪ من العينة، مما يشير إلى أن ما يقارب نصف العينة هم من الشباب في هذا العمر، تأتي الفئة العمرية

من ٣٠ إلى ٤٠ سنة في المرتبة الثانية، حيث تشكل ٤٣٪ من العينة. يليها الفئة العمرية الأقل من ٢٠ سنة التي تمثل جزءاً صغيراً أيضاً. وتبقى الفئة العمرية الأكبر من ٤٠ سنة هي الأقل تمثيلاً في العينة، مما يشير إلى انخفاض نسبة الأفراد الأكبر سناً في هذه العينة المحددة.

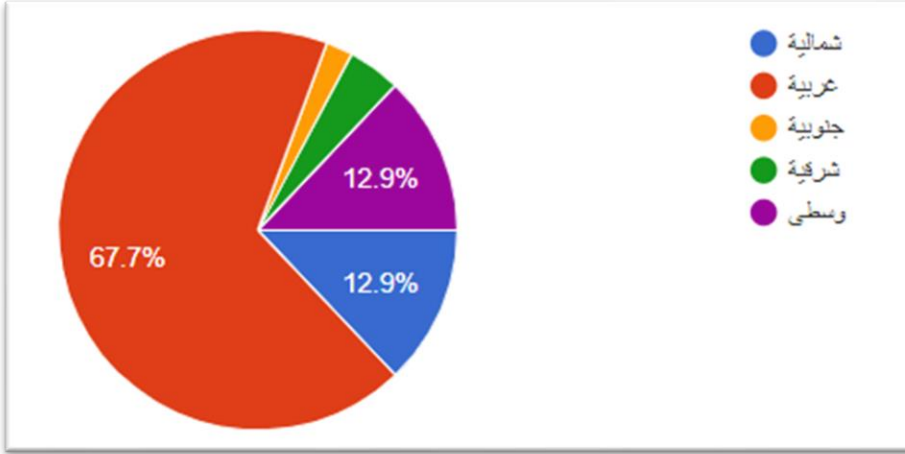
■ الجنس

شكل (٣-٢): معلومات الجنس

يظهر في التوزيع تباين واضح في نسب التمثيل بين الذكور والإناث. يمثل الذكور نسبة ٢٢.٨٪ من العينة، بينما تمثل الإناث النسبة الأكبر بواقع ٧٧.٢٪.



■ المنطقة الجغرافية



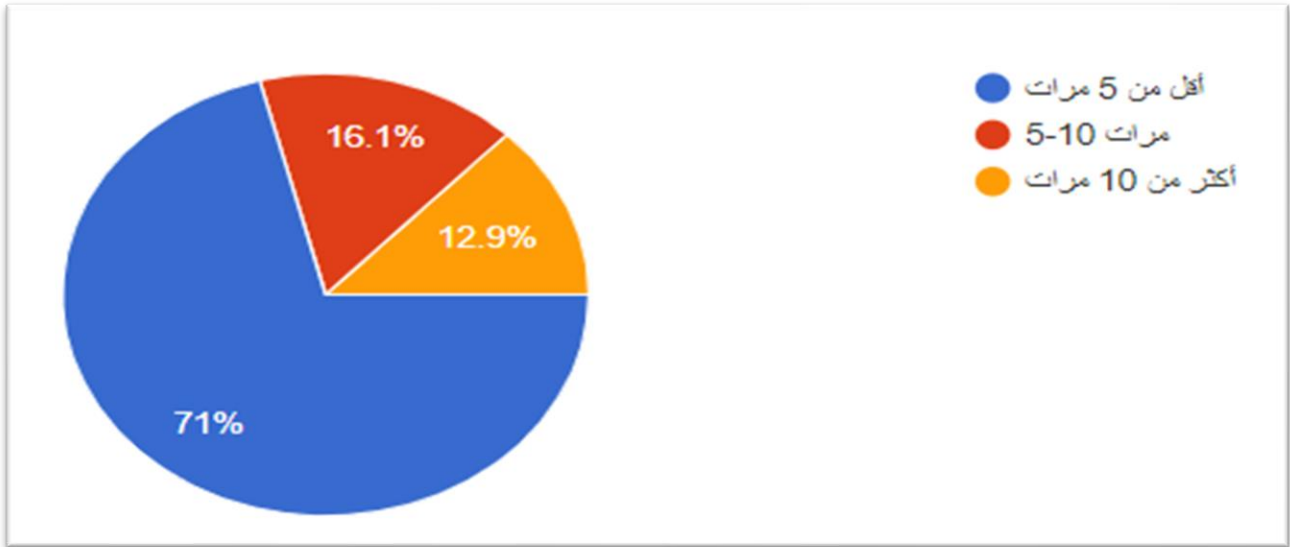
شكل (٣-٣): معلومات المنطقة الجغرافية

المنطقة الغربية: تشكل

النسبة الأكبر بواقع ٦٧.٧٪ من العينة، مما يشير إلى أن غالبية الأفراد في العينة يأتون من هذه

المنطقة. بينما المنطقة الشمالية تمثل ١٢.٩٪ من العينة، وهي نسبة مساوية للمنطقة الوسطى. بينما المنطقة الشرقية والجنوبية تمثلان نسبة صغيرة جداً من العينة.

ثانياً : أسئلة الاستبيان



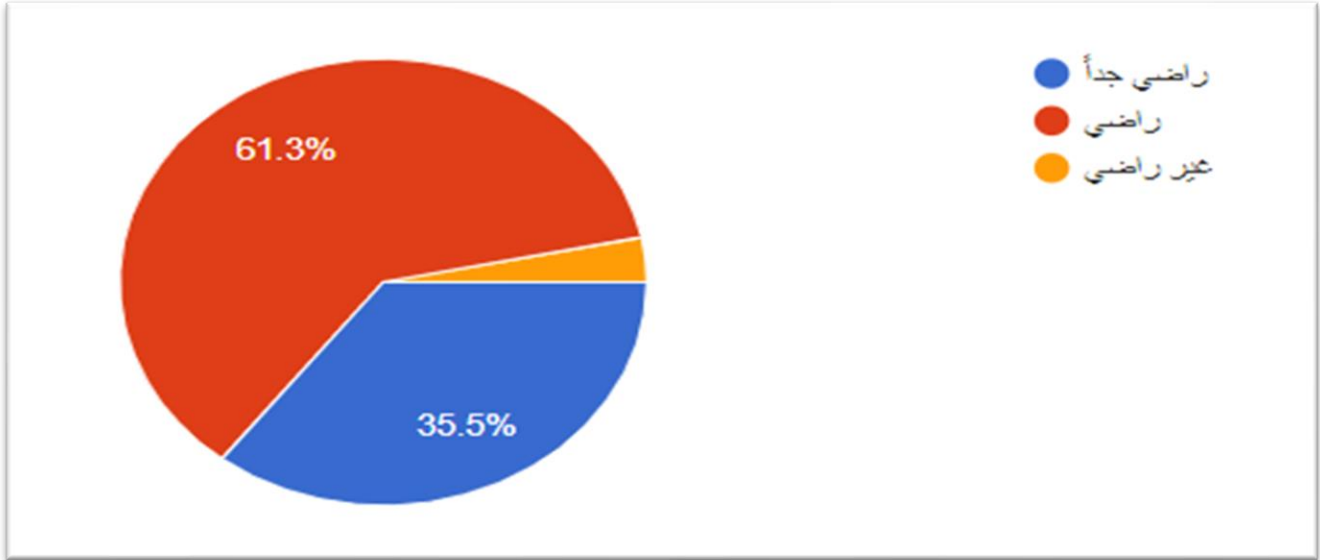
شكل (٣-٤): يوضح عدد مرات استخدام تطبيق جاهز في الشهر

يوضح الاجابات أن الأغلبية الساحقة من المستخدمين يستعملون التطبيق أقل من ٥ مرات في الشهر، بنسبة تصل إلى ٧١٪. هذا يشير إلى أن معظم المستخدمين قد يكونون غير معتمدين بشكل كبير على التطبيق في حياتهم اليومية

في المقابل، نجد أن ١٦.١٪ من المستخدمين يستعملون التطبيق بين ٥ إلى ١٠ مرات في الشهر، مما يعكس مستوى متوسط من الاستخدام، قد يرتبط بالأشخاص الذين يعتمدون على التطبيق بشكل منتظم ولكن ليس يومياً.

أما الفئة التي تستخدم التطبيق أكثر من ١٠ مرات في الشهر، فتشكل ١٢.٩٪ من العينة. هذه الفئة قد تضم المستخدمين الذين يعتمدون على التطبيق بشكل كبير ومتكرر، ربما نتيجة لاحتياجاتهم اليومية وتفضيلهم لخدمات التطبيق بشكل مستمر.

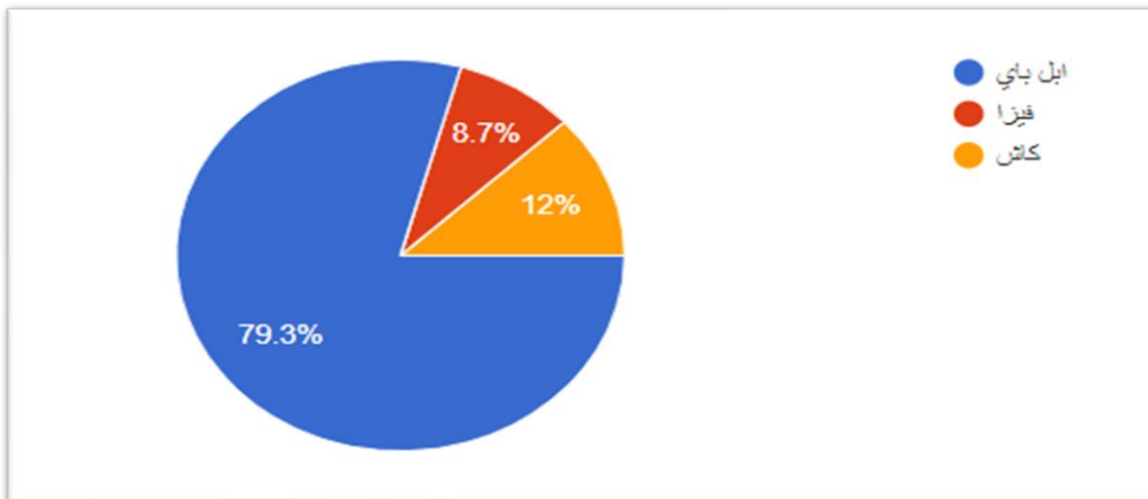
ما مدى رضاك عن سرعة توصيل الطلبات عبر تطبيق " جاهز " ؟



شكل (٣-٥): يوضح مدى الرضا عن سرعة توصيل الطلبات

توضح الاجابات ان هناك مستوى عالي من الرضا بين المستخدمين. حيث أن ٣٥.٥٪ من المستخدمين أبدوا رضاهم الشديد عن سرعة التوصيل، ونجد أن ٦١.٣٪ من المستخدمين يشعرون بالرضا عن سرعة التوصيل، مما يعني أن الغالبية العظمى من المستخدمين راضون بشكل عام عن الخدمة المقدمة. هذا يدل على أن التطبيق ينجح في تلبية توقعات العملاء في معظم الحالات. من ناحية أخرى، فقط ٣.٢٪ من المستخدمين أعربوا عن عدم رضاهم عن سرعة التوصيل. هذه النسبة الضئيلة تشير إلى أن هناك عدد قليل من المستخدمين الذين قد يواجهون مشاكل أو تأخيرات في توصيل طلباتهم،

طريقة الدفع المستخدمة



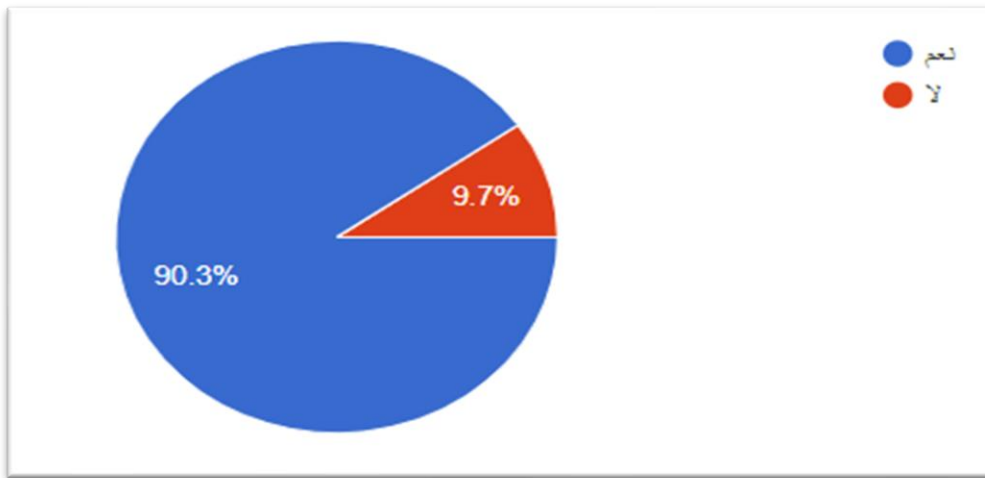
شكل (٣-٦):

يوضح طريقة الدفع المستخدمة

ابل باي تمثل الطريقة الأكثر استخدامًا بنسبة ٧٩.٣٪. هذا يشير إلى أن الغالبية العظمى من المستخدمين يفضلون استخدام الدفع الإلكتروني عبر Apple Pay، ربما بسبب سهولة الاستخدام والأمان الذي توفره هذه الطريقة. بينما بطاقات فيزا: تمثل ٨.٧٪ من المستخدمين، وهي نسبة صغيرة مقارنة بابل باي. أما الدفع النقدي (كاش): يستخدمه فئة قليل جداً بنسبة ١٢٪

بشكل عام، تظهر البيانات أن هناك تفضيلاً كبيراً للدفع الإلكتروني عبر Apple Pay بين مستخدمي تطبيق "جاهز"، مما يعكس التحول نحو التكنولوجيا المالية الحديثة والابتعاد عن الطرق التقليدية مثل الدفع النقدي.

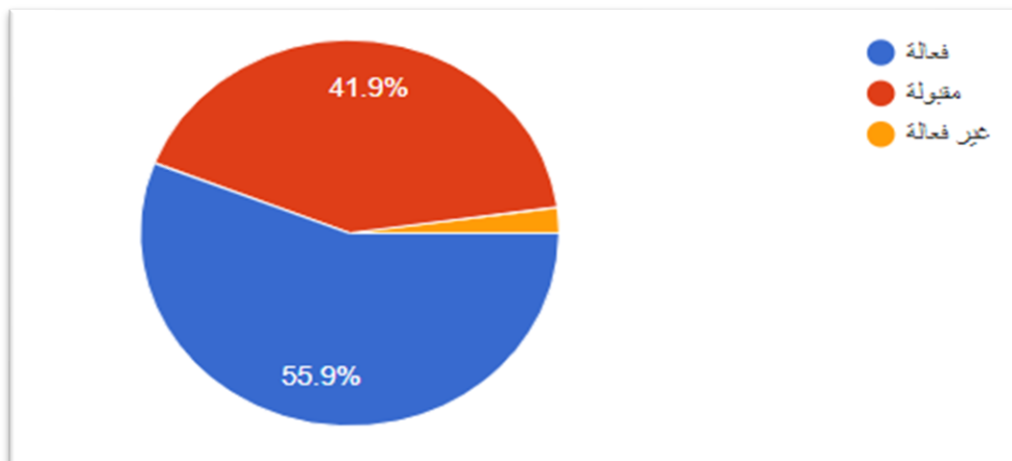
هل تشعر أن بياناتك الشخصية آمنة عند استخدام تطبيق " جاهز " ؟



شكل (٣-٧): هل البيانات آمنة عند استخدام تطبيق جاهز

توضح الإجابات أن الغالبية العظمى من المستخدمين يشعرون بأن بياناتهم الشخصية آمنة عند استخدام التطبيق. هذا يشير إلى أن الغالبية العظمى من المستخدمين لديهم ثقة كبيرة في إجراءات الأمان والخصوصية التي يتبعها التطبيق. تعكس البيانات مستوى عالياً من الثقة بين المستخدمين في حماية بياناتهم الشخصية عند استخدام تطبيق "جاهز"، مما يعزز من سمعة التطبيق ويزيد من قاعدة مستخدميه. الحفاظ على هذه الثقة من خلال الاستمرار في تحسين إجراءات الأمان وتوفير الشفافية للمستخدمين سيكون له تأثير إيجابي.

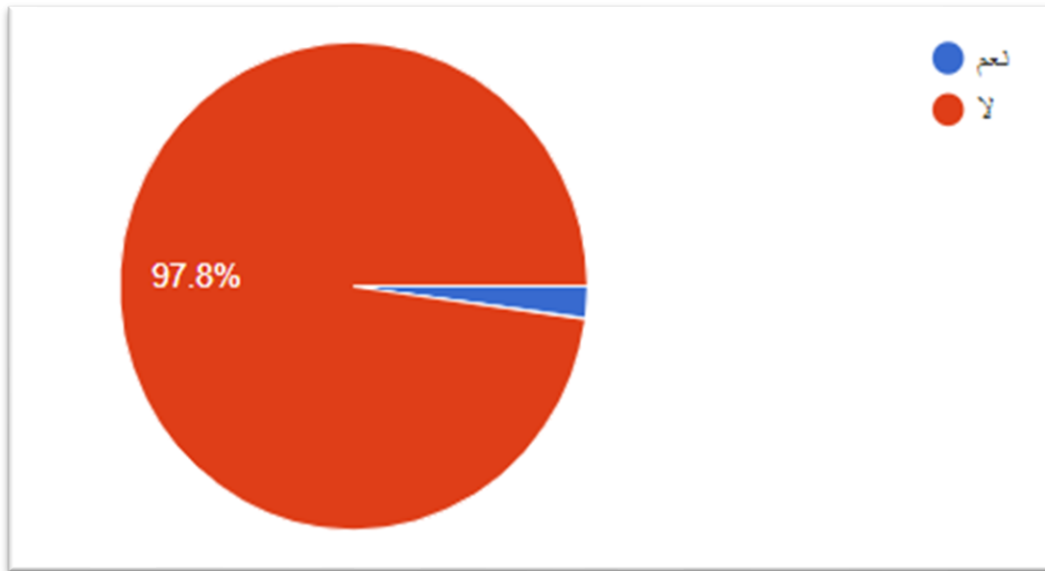
كيف تقيم فعالية الإجراءات الأمنية التي يتبعها تطبيق " جاهز " لحماية معلومات الشخصية؟



شكل (٣-٨): تقييم فعالية الإجراءات الأمنية في تطبيق جاهز

تشير الاجابات إلى أن هناك مستوى جيدا من الرضا عن هذه الإجراءات حيث ان ٥٥.٩٪ من المستخدمين يرون أن الإجراءات الأمنية التي يتبعها التطبيق لحماية معلوماتهم الشخصية فعالة. هذا يعكس رضا وثقة كبيرة من قبل أكثر من نصف المستخدمين في قدرة التطبيق على حماية بياناتهم الشخصية بشكل جيد. بينما ٤١.٩٪ من المستخدمين يعتبرون أن الإجراءات الأمنية مقبولة. هذه النسبة الكبيرة تشير إلى أن هناك مستوى معين من الرضا، ولكن يمكن أن تكون هناك بعض التحسينات المطلوبة لرفع مستوى الثقة إلى "فعالة" لدى هؤلاء المستخدمين. اما ٢.٢٪ من المستخدمين يرون أن الإجراءات الأمنية غير فعالة. هذه النسبة الصغيرة تمثل فئة من المستخدمين الذين قد يكون لديهم مخاوف أو تجارب سلبية بشأن حماية بياناتهم.

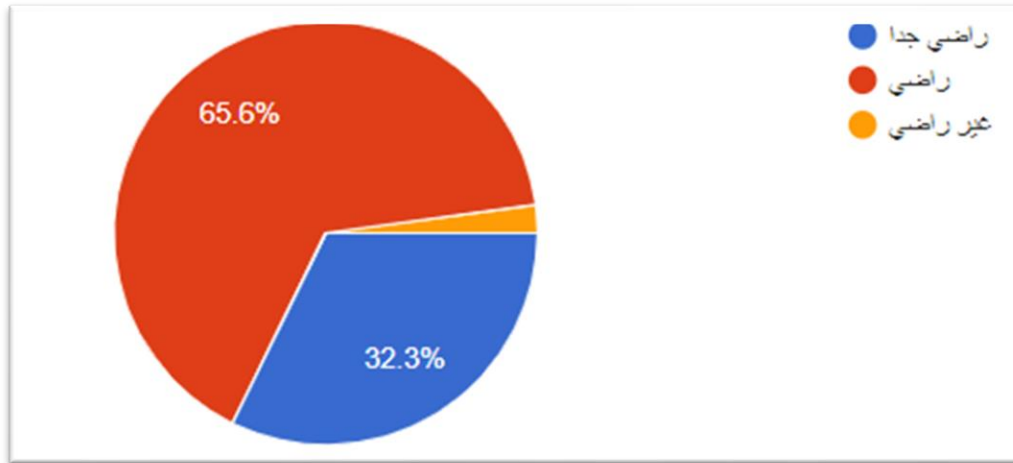
هل سبق أن واجهت أي مشاكل أمنية (مثل تسرب البيانات أو احتيال) عند استخدام التطبيق؟



شكل (٣-٩): توضيح
اي مشاكل امنيه واجهه
المستخدم عند استخدام
التطبيق

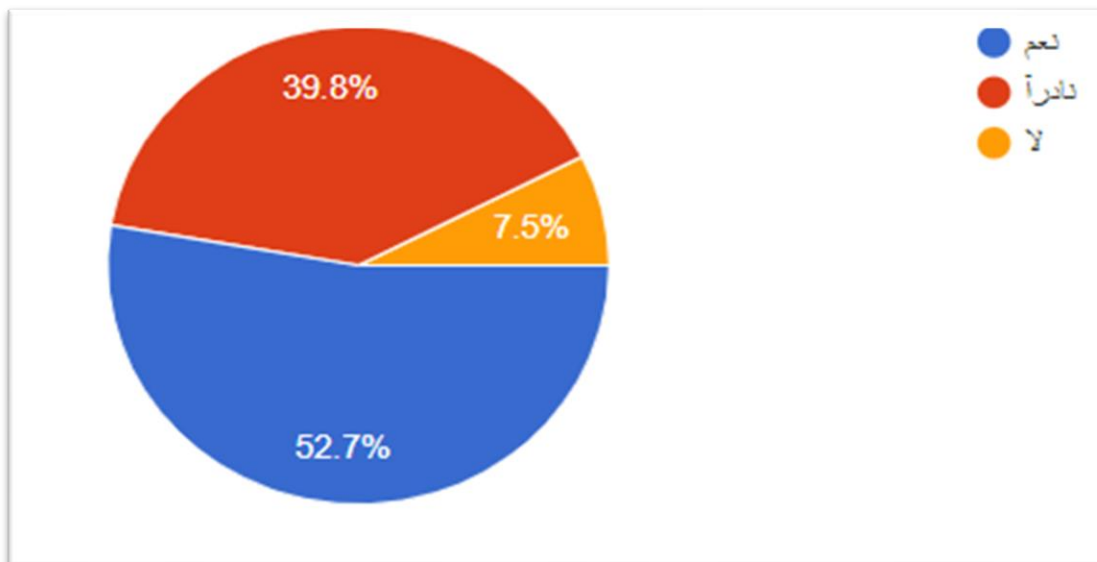
تشير الاجابات إلى أن الغالبية العظمى لم يواجهوا أي مشاكل أمنية حيث ان ٩٧.٨٪ من المستخدمين لم يواجهوا أي مشاكل أمنية مثل تسريب البيانات أو الاحتيال عند استخدام التطبيق. هذه النسبة العالية تعكس فعالية الإجراءات الأمنية التي يتبعها التطبيق، وتعزز الثقة الكبيرة بين المستخدمين فيما يتعلق بحماية بياناتهم الشخصية. بينما ٢.٢٪ فقط من المستخدمين واجهوا مشاكل أمنية. على الرغم من أن هذه النسبة ضئيلة إلا أنها تشير إلى وجود بعض الحالات التي قد تستدعي اهتماماً وتحليلاً أعمق من قبل فريق الأمان في التطبيق. معالجة هذه القضايا وتعزيز التدابير الأمنية يمكن أن يساعد في تقليل هذه النسبة إلى الصفر.

ما مدى رضاك عن جودة الخدمات المقدمة من خلال التطبيق (مثل دقة الطلبات ، حالة المنتجات عند التوصيل) ؟



شكل (٣-١٠): توضيح مدى رضا المستخدمين عن جودة الخدمات المقدمة من خلال التطبيق
تشير الاجابات إلى مستويات عالية من الرضا بين المستخدمين حيث ان راضي جداً مثلت ٣٢.٣% من المستخدمين يشعرون برضا كبير عن جودة الخدمات المقدمة. هذه النسبة تعكس تقديراً عالياً للخدمات التي يقدمها التطبيق، بينما راضي مثلت النسبة الأعلى حيث ان ٦٥.٦% من المستخدمين يعبرون عن رضاهم عن جودة الخدمات. هذه النسبة الكبيرة تشير إلى أن معظم المستخدمين راضون عن الخدمات المقدمة ، بينما غير راضي مثلت ٢.٢% من المستخدمين غير راضين عن جودة الخدمات المقدمة.

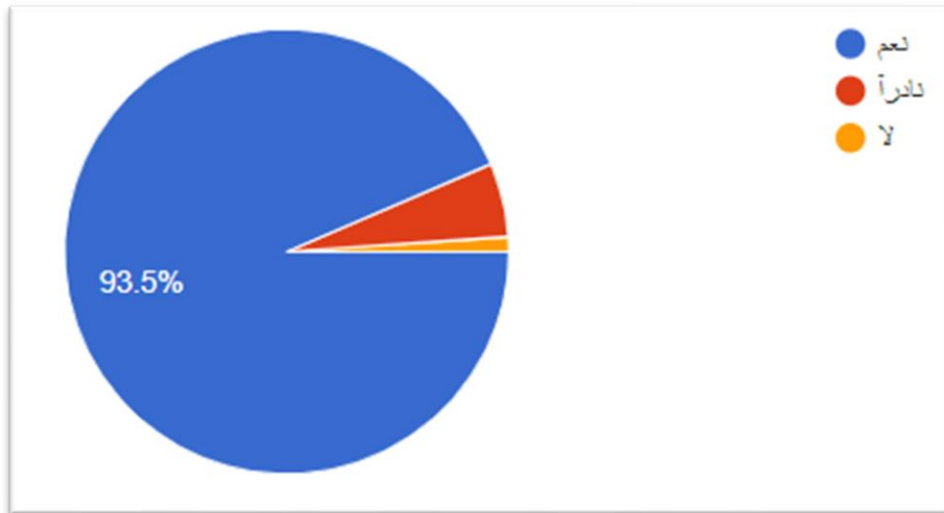
هل تلاحظ تحديثات وتحسينات دورية في تطبيق " جاهز " ؟



شكل (٣-١١): ملاحظة وجود تحديثات وتحسينات دورية في تطبيق جاهز
تشير الاجابات إلى تباين في مدى انتباه المستخدمين لهذه التحديثات. التحليل التالي يوضح هذه النتائج:

- نعم: ٥٢.٧% من المستخدمين يلاحظون التحديثات والتحسينات الدورية في التطبيق. هذه النسبة تعكس إدراكًا جيدًا لجهود الفريق المطور في تحسين وتطوير التطبيق باستمرار، مما يعزز من تجربة المستخدمين ويزيد من رضاهم.
 - نادرًا: ٣٩.٨% من المستخدمين يلاحظون التحديثات بشكل نادر. هذا يشير إلى أن هناك شريحة كبيرة من المستخدمين الذين قد لا يكونون على دراية بالتحديثات أو أنهم لا يلاحظون الفروق بشكل واضح. يمكن أن يكون هذا ناتجًا عن عدم وضوح التحسينات أو عدم توفير معلومات كافية حولها للمستخدمين.
 - لا: ٧.٥% من المستخدمين لا يلاحظون أي تحديثات أو تحسينات دورية في التطبيق. هذه النسبة الصغيرة تشير إلى وجود فئة من المستخدمين الذين قد يشعرون بأن التطبيق يفتقر إلى التطوير المستمر، مما قد يؤثر على رضاهم وتجربتهم مع التطبيق.
- تعكس البيانات أن هناك وعيًا جيدًا بين المستخدمين بجهود التحسين المستمرة في تطبيق "جاهز"، ولكن هناك مجال لتعزيز هذا الوعي من خلال تحسين التواصل مع المستخدمين وتوضيح الفوائد والمزايا الناتجة عن التحديثات الدورية.

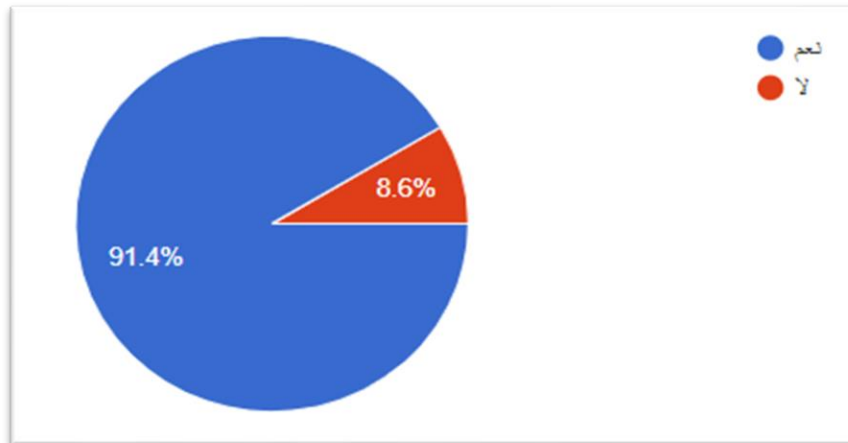
هل تتلقى اشعارات كافية حول حالة طلبك (مثل تأكيد الطلب ، الشحن ، التوصيل) ؟



شكل (٣-١٢): توضيح حول تلقي اشعارات كافية حول طلبك

تشير الاجابات إلى أن الأغلبية العظمى من المستخدمين راضون عن مستوى الإشعارات المقدمة حيث تعكس الاجابات أن تطبيق "جاهز" يقدم نظام إشعارات فعال وموثوق به لمعظم المستخدمين، مما يساهم في تحسين تجربة الطلب والتوصيل. الاستمرار في تحسين وتطوير نظام الإشعارات يمكن أن يضمن رضا جميع المستخدمين ويعزز من سمعة التطبيق كخدمة موثوقة وفعالة.

هل توصي الآخرين باستخدام تطبيق " جاهز " ؟



شكل (٣-١٣): توضيح حول توصي الآخرين باستخدام تطبيق جاهز

تشير الاجابات الى مستوى عالي من الرضا والثقة بين المستخدمين، مما يعزز من سمعة التطبيق ويزيد من احتمالية نمو قاعدة مستخدميه من خلال التوصيات الشفوية.

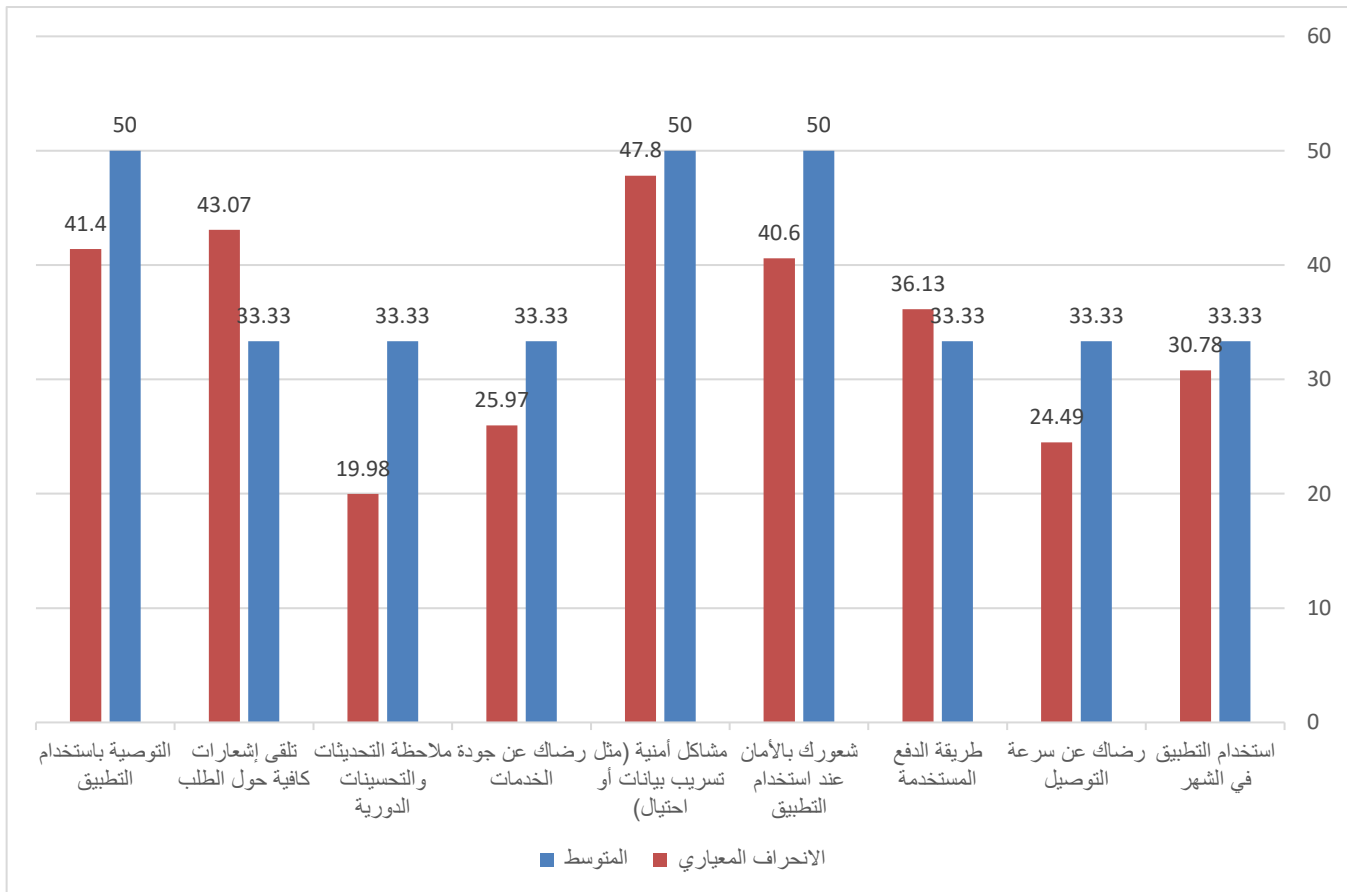
جدول المتوسط والانحراف المعياري

جدول (٣-١): جدول المتوسط والانحراف المعياري

الانحراف المعياري	المتوسط	النسبة (%)	الفئة
30.78	33.33		استخدام التطبيق في الشهر
		71	أقل من ٥ مرات
		16.1	5-10 مرات
		12.9	أكثر من ١٠ مرات
24.49	33.33		رضاك عن سرعة التوصيل
		35.5	راضي جداً
		61.3	راضي
		3.2	غير راضي
36.13	33.33		طريقة الدفع المستخدمة
		79.3	Apple Pay
		8.7	Visa
		12	كاش
40.6	50		شعورك بالأمان عند استخدام التطبيق
		90.3	نعم
		9.7	لا
22.46	33.33		فعالية الإجراءات الأمنية
		55.9	فعالة
		41.9	مقبولة
		2.2	غير فعالة
47.8	50		مشاكل أمنية (مثل تسريب بيانات أو احتيال)
		2.2	نعم
		97.8	لا
25.97	33.33		رضاك عن جودة الخدمات
		32.3	راضي جداً
		65.6	راضي
		2.2	غير راضي

الفئة	النسبة (%)	المتوسط	الانحراف المعياري
ملاحظة التحديثات والتحسينات الدورية		33.33	19.98
نعم	52.7		
نادرًا	39.8		
لا	7.5		
تلقى إشعارات كافية حول الطلب		33.33	43.07
نعم	93.5		
نادرًا	5.4		
لا	1.1		
التوصية باستخدام التطبيق		50	41.4
نعم	91.4		
لا	8.6		

شكل (٣-١٤): مخطط يوضح المتوسط والانحراف المعياري



الفصل الرابع: النتائج والتوصيات

النتائج :

• استخدام التطبيق وتكراره:

غالبية المستخدمين يستخدمون التطبيق بشكل متفاوت، ومعظمهم يستخدمه أقل من ٥ مرات في الشهر، مما يشير إلى أهمية تعزيز الاستخدام المتكرر وزيادة التفاعل.

• رضا المستخدم عن سرعة التوصيل:

تظهر نسب عالية من الرضا بشكل عام، حيث يشعر غالبية المستخدمين بالرضا أو الرضا الكامل بسرعة التوصيل.

• طرق الدفع المستخدمة:

طريقة الدفع المفضلة بين المستخدمين هي Apple Pay، مما يوحي بالرغبة في تبسيط وتسريع عمليات الدفع الرقمية.

• الأمان والثقة:

غالبية المستخدمين يشعرون بالأمان عند استخدام التطبيق، لكن هناك حاجة مستمرة لتعزيز الأمان وزيادة الوعي بالمخاطر الإلكترونية المحتملة.

• فعالية الإجراءات الأمنية:

الأغلبية تعتبر الإجراءات الأمنية المعتمدة من قبل التطبيق فعالة، ولكن هناك فرصة لتحسينها لتعزيز الثقة والحماية.

• جودة الخدمات المقدمة:

معظم المستخدمين راضون عن جودة الخدمات المقدمة، مما يعكس التزام التطبيق بتحقيق التميز في تجربة المستخدم.

• تحديثات وتحسينات دورية:

الأغلبية تلاحظ وتقيم التحديثات والتحسينات الدورية، مما يعزز من قدرة التطبيق على التكيف مع احتياجات المستخدمين والتطورات التكنولوجية.

مناقشة النتائج :

• استخدام التطبيق:

النتيجة تظهر أن معظم المستخدمين يستخدمون التطبيق بشكل متكرر، مع تفاوت في عدد الاستخدامات الشهرية. هذا يشير إلى الفرصة في تحفيز المستخدمين للتفاعل المتكرر مع التطبيق من خلال برامج ولاء وعروض خاصة.

• رضا المستخدم عن سرعة التوصيل:

الرضا العالي من المستخدمين بشأن سرعة التوصيل يعكس التركيز الناجح على تحسين اللوجستيات وتقديم خدمات سريعة وفعالة.

- **أمان البيانات والثقة:**

رغم أن غالبية المستخدمين يشعرون بالأمان، إلا أن هناك حاجة لزيادة الجهود في تعزيز الأمان الإلكتروني وزيادة الوعي بأهمية حماية البيانات الشخصية.

- **فعالية الإجراءات الأمنية:**

الإجراءات الأمنية المعتمدة حالياً تعتبر فعالة من وجهة نظر الغالبية، ولكن هناك فرصة لتحسينها لتعزيز الثقة والحماية.

- **جودة الخدمات المقدمة:**

معظم المستخدمين يظهرون رضاً جيداً عن جودة الخدمات المقدمة، وهذا يعكس التزام التطبيق بتقديم تجربة مستخدم مرضية وموثوقة.

التوصيات :

بناء على النتائج المستخلصة يمكن اقتراح التوصيات التالية:

- **تعزيز الاستخدام المتكرر:**

تقديم برامج ولاء وعروض خاصة للمستخدمين الذين يستخدمون التطبيق بشكل متكرر لزيادة عدد الطلبات الشهرية.

- **تحسين سرعة التوصيل:**

تحسين العمليات اللوجستية وتقليل وقت الانتظار لتعزيز رضا العملاء عن سرعة التوصيل.

- **توسيع خيارات الدفع:**

توفير مزيد من خيارات الدفع الرقمي والنقدي لتلبية تفضيلات المستخدمين وتعزيز سهولة الدفع.

- **تعزيز الأمان والثقة:**

تعزيز الأمان من خلال تحسين إجراءات حماية البيانات وزيادة الوعي بأهمية الأمان الإلكتروني بين المستخدمين.

- **تحسين فعالية الإجراءات الأمنية:**

تحسين الإجراءات الأمنية لزيادة فعاليتها وتعزيز الثقة بين المستخدمين في حماية بياناتهم الشخصية.

- **تحسين جودة الخدمات المقدمة:**

استمرار في تحسين جودة الخدمات المقدمة لزيادة رضا المستخدمين وتعزيز التفاعل الإيجابي مع التطبيق.

- **تركيز للتحديثات والتحسينات الدورية:**

استمرار في تقديم التحديثات والتحسينات الدورية للتطبيق لضمان التكيف مع تطورات المستخدمين والتطورات

التكنولوجية.

- **تعزيز التواصل والشفافية:**

تقديم معلومات دورية وشفافة للمستخدمين حول التحديثات والتغييرات في التطبيق والإجراءات الأمنية لبناء الثقة وتعزيز التفاعل الإيجابي.

مناقشة التوصيات :

- تحفيز الاستخدام المتكرر:

تقديم مزيد من الحوافز والعروض الخاصة للمستخدمين الذين يستخدمون التطبيق بانتظام لزيادة عدد الطلبات الشهرية.

- تحسين التواصل والشفافية:

زيادة التواصل مع المستخدمين حول التحديثات والتحسينات في التطبيق، بالإضافة إلى توفير معلومات دقيقة حول خدمات التوصيل والدفع.

- تعزيز الأمان والحماية:

تحسين إجراءات حماية البيانات وزيادة التوعية بالمخاطر الإلكترونية لتعزيز الثقة بين المستخدمين والحفاظ على سمعة التطبيق.

- استمرار في التحسينات الدورية:

الاستمرار في تقديم التحديثات والتحسينات الدورية للتطبيق للتكيف مع تطورات السوق واحتياجات المستخدمين.

- تحسين تجربة المستخدم بشكل عام:

التركيز على تحسين جودة الخدمات المقدمة وتبسيط عمليات الدفع والتوصيل لزيادة رضا المستخدم والولاء للتطبيق.

الخاتمة

في هذه الدراسة، تم تحليل دور إدارة المخاطر الرقمية في تشغيل تطبيقات التوصيل باستخدام تطبيق "جاهز" كنموذج. استندت الدراسة إلى منهجية تجمع بين الأساليب الكمية والنوعية، حيث تم جمع البيانات من خلال استبيانات ومقابلات مع مستخدمي التطبيق والعاملين فيه. هدفت الدراسة إلى فهم تأثير إدارة المخاطر الرقمية على كفاءة وأمان تشغيل التطبيقات وتحسين تجربة المستخدم.

أبرز النتائج :

١. عدد مرات استخدام التطبيق:

- أظهرت البيانات أن ٧١٪ من المستخدمين يستخدمون التطبيق أقل من ٥ مرات في الشهر، مما يشير إلى استخدام غير منتظم نسبياً للتطبيق بين غالبية المستخدمين.

٢. رضا المستخدم عن سرعة التوصيل:

- كانت نسبة الرضا عن سرعة التوصيل مرتفعة، حيث عبر ٩٦.٨٪ من المستخدمين عن رضاهم (راضون أو راضون جداً)، مما يعكس فعالية الخدمات اللوجستية للتطبيق.

٣. طريقة الدفع المستخدمة:

- أظهرت النتائج تفضيلاً كبيراً للدفع الإلكتروني عبر Apple Pay بنسبة ٧٩.٣٪، مما يشير إلى تحول نحو الدفع الرقمي بين مستخدمي التطبيق.

٤. الأمان والثقة:

- شعر ٩٠.٣٪ من المستخدمين بالأمان عند استخدام التطبيق، مما يعكس فعالية إجراءات الأمان المتبعة في "جاهز".

٥. فعالية الإجراءات الأمنية:

- اعتبر ٩٧.٨٪ من المستخدمين أن الإجراءات الأمنية في التطبيق فعالة أو مقبولة، مما يعزز الثقة في التطبيق وقدرته على حماية بيانات المستخدمين.

٦. جودة الخدمات المقدمة:

- أبدى ٩٧.٩٪ من المستخدمين رضاهم عن جودة الخدمات المقدمة، مما يعكس التزام التطبيق بتقديم تجربة مستخدم مرضية.

٧. التحديثات والتحسينات الدورية:

- لاحظ ٩٢.٥٪ من المستخدمين وجود تحديثات وتحسينات دورية في التطبيق، مما يشير إلى التزام "جاهز" بتحسين الخدمات باستمرار.

التوصيات :

بناءً على النتائج المستخلصة، يمكن اقتراح التوصيات التالية:

- (١) تقديم برامج ولاء وعروض خاصة للمستخدمين الذين يستخدمون التطبيق بشكل متكرر لزيادة عدد الطلبات الشهرية.

- ٢) تحسين العمليات اللوجستية وتقليل وقت الانتظار لتعزيز رضا العملاء عن سرعة التوصيل.
 - ٣) توفير مزيد من خيارات الدفع الرقمي والنقدي لتلبية تفضيلات المستخدمين وتعزيز سهولة الدفع.
 - ٤) تعزيز الأمان من خلال تحسين إجراءات حماية البيانات وزيادة الوعي بأهمية الأمان الإلكتروني بين المستخدمين.
 - ٥) تحسين الإجراءات الأمنية لزيادة فعاليتها وتعزيز الثقة بين المستخدمين في حماية بياناتهم الشخصية.
 - ٦) الاستمرار في تحسين جودة الخدمات المقدمة لزيادة رضا المستخدمين وتعزيز التفاعل الإيجابي مع التطبيق.
 - ٧) الاستمرار في تقديم التحديثات والتحسينات الدورية للتطبيق لضمان التكيف مع تطلعات المستخدمين والتطورات التكنولوجية.
 - ٨) تقديم معلومات دورية وشفافة للمستخدمين حول التحديثات والتغييرات في التطبيق والإجراءات الأمنية لبناء الثقة وتعزيز التفاعل الإيجابي.
- ونختم القول إن هذه الدراسة تمثل خطوة مهمة نحو فهم إدارة المخاطر الرقمية في تطبيقات التوصيل، وقدمت رؤى قيمة حول كيفية تحسين الأمان والكفاءة لتطبيق "جاهز". من خلال تنفيذ التوصيات المقدمة، يمكن للتطبيق تعزيز تجربته للمستخدمين وزيادة ثقته بهم، مما يعزز نجاحه واستمراره في السوق.

المراجع

- إبراهيم، ميسون. ٢٠٢٣. "مخاطر التكنولوجيا الرقمية الحديثة في الخليج: المشاكل والحلول" آراء حول الخليج، ع ١٨٤: ٧٩-٨٣. مركز الخليج للبحوث.
- ابن يوب، شمس الجميلي وبلقي، نور نزوان. ٢٠٢٢. "تطبيقات توصيل الطعام وعباراتها وسياقاتها: دراسة تحليلية سيميائية". مجلة الدراسات اللغوية والأدبية، س ١٣، ع ٢: ٧٦-٩٧. الجامعة الإسلامية العالمية.
- إحليل، كريم. ٢٠٢٤. "الأمن السيبراني". المجلة الإلكترونية الدولية للقانون القانوني، مج ٤، ع ١٨: ٤٨-٧٤. مصطفى الغشام الشعبي.
- أبو عتيقة، ضرغام عبدالله فاضل. ٢٠٢١. "حماية بيانات الشخصية عبر شبكة الإنترنت: دراسة مقارنة". رسالة ماجستير غير منشورة، الجامعة الأردنية، عمان، الأردن.
- دحماني، محمد. ٢٠٢٣. "التحديات السيبرانية: الهندسة الاجتماعية أنموذجاً". المجلة الأكاديمية للبحوث القانونية والسياسية، مج ٧، ع ٢: ٦٨١-٧٠١. جامعة عمار ثلجي الأغواط - كلية الحقوق والعلوم النفسية.
- جراح، ندى بدر. ٢٠٠٩. "تقنيات الترجمة في الترجمة التجارية الإلكترونية". مجلة ميسان للدراسات الأكاديمية، مج ٧، ع ١٤: ١٩٣-٢١٠. جامعة ميسان - كلية التربية الأساسية.
- علي، اسراء عبدالقادر حسن محمد. ٢٠١٦. "نظام دعم فني للمشاكل التقنية". رسالة ماجستير غير منشورة، جامعة النيلين، الخرطوم، السودان.
- أحرز الله، عبدالكريم. ٢٠١٩. "التعلم الآلي جزء من الذكاء الاصطناعي". مجلة العلوم والتكنولوجيا المجلس الأعلى للغة العربية: ١٣-٢٨.
- مرسي، نورهان سامي فتح الله. ٢٠٢٣. "تجربة المستخدم من ذوي الاحتياجات الخاصة بالمواقع الإلكترونية للجامعات المصرية". المجلة العربية الدولية لدراسات المكتبات الخاصة، المؤسسة العربية للمعرفة، مج ٢، ع ١١٥: ٢-١٤٤.
- الغرابوي، محمد أحمد أمين أحمد. ٢٠٢٢. "أثر تطبيقات الهاتف المحمول على القيمة المدركة لعملاء تطبيقات الطعام توصيل بالمملكة العربية السعودية". مجلة التجارة والتمويل، جامعة طنطا - كلية التجارة، ع ٢: ١٥٩-٢٣٠.
- أحمد حمدي ودبا، النحاس ندى طارق. (٢٠٢٢). "إدارة التحول الرقمي". المجلة العلمية والبحوث العلمية والإدارية، المجلد ١٣ (ملحق)، صص ١٥٠١-١٥١٣.
- العتيبي، نورة بنت عمر. (٢٠٢٣). "العمل في منصات النقل التشاركي: الفرص والتحديات: دراسة وصفية تحليلية من قسم العاملين في تطبيقات النقل والأجرة وتوصيل الطعام". مجلة الخدمة الاجتماعية، المجلد ٧٥، العدد ٢، صص ٢٣٤-٢٥٠.
- محمد، سماح (٢٠٢٠). بناء تطبيق أندرويد لطلب الوجبات بالطب على مطعم السماكة [رسالة ماجستير غير منشورة]. كلية الدراسات العليا، جامعة النيلين، الخرطوم، السودان.

- العموش، م.ح. (٢٠٢١). تأثير تطبيقات توصيل الطعام على الأداء التسويقي للمطاعم في الأردن: دراسة حالة تطبيق مايسترو في مدينة المفرق. [رسالة ماجستير غير منشورة]. كلية الاقتصاد والعلوم الإدارية، جامعة آل البيت، المفرق، الأردن.
- العموش، م.ح. (٢٠٢١). تأثير تطبيقات توصيل الطعام على الأداء التسويقي للمطاعم في الأردن: دراسة حالة تطبيق مايسترو في مدينة المفرق. [رسالة ماجستير غير منشورة]. كلية الاقتصاد والعلوم الإدارية، جامعة آل البيت، المفرق، الأردن.

الملاحق

أسئلة الاستبانة المستخدمة في هذه الدراسة
المعلومات الديموغرافية

١. العمر:

- أقل من ٢٠ سنة
- من ٢٠ إلى ٢٩ سنة
- من ٣٠ إلى ٣٩ سنة
- من ٤٠ إلى ٤٩ سنة
- 50 سنة فأكثر

٢. الجنس:

- ذكر
- أنثى

٣. المنطقة الجغرافية:

- المنطقة الغربية
- المنطقة الوسطى
- المنطقة الشرقية
- المنطقة الشمالية
- المنطقة الجنوبية

استخدام التطبيق وتجربة المستخدم

٤. كم مرة تستخدم تطبيق "جاهز" في الشهر؟:

- أقل من ٥ مرات
- من ٥ إلى ١٠ مرات
- أكثر من ١٠ مرات

٥. ما مدى رضاك عن سرعة توصيل الطلبات عبر تطبيق "جاهز"؟:

- راضٍ جداً
- راضٍ
- غير راضٍ

٦. ما هي طريقة الدفع التي تستخدمها عادة عند الطلب من تطبيق "جاهز"؟:

- Apple Pay
- بطاقة Visa
- نقداً (كاش)

٧. هل تشعر أن بياناتك الشخصية آمنة عند استخدام تطبيق "جاهز"؟:

- نعم
- لا

٨. كيف تقيم فعالية الإجراءات الأمنية التي يتبعها تطبيق "جاهز" لحماية معلوماتك الشخصية؟:

- فعالة جداً
- مقبولة
- غير فعالة

٩. هل سبق أن واجهت أي مشاكل أمنية (مثل تسريب البيانات أو الاحتيال) عند استخدام التطبيق؟:

- نعم
- لا

١٠. ما مدى رضاك عن جودة الخدمات المقدمة من خلال التطبيق (مثل دقة الطلبات، حالة المنتجات عند التوصيل)؟:

- راضٍ جداً
- راضٍ
- غير راضٍ

١١. هل تلاحظ تحديثات وتحسينات دورية في تطبيق "جاهز"؟:

- نعم
- نادراً
- لا

١٢. هل تتلقى إشعارات كافية حول حالة طلبك (مثل تأكيد الطلب، الشحن، التوصيل)؟:

- نعم
- نادراً
- لا

١٣. هل توصي الآخرين باستخدام تطبيق "جاهز"؟:

- نعم
- لا

جدول (٤-١) : يوضح توزيع الإجابات على الأسئلة المختلفة

السؤال	الفئات	النسبة المئوية (%)
عدد مرات استخدام التطبيق في الشهر	أقل من ٥ مرات	71.0
	5-10 مرات	16.1
	أكثر من ١٠ مرات	12.9
مدى رضاك عن سرعة التوصيل	راضي جداً	35.5
	راضي	61.3
	غير راضي	3.2
طريقة الدفع المستخدمة	Apple Pay	79.3
	Visa	8.7
	كاش	12.0
شعورك بالأمان عند استخدام التطبيق	نعم	90.3
	لا	9.7
فعالية الإجراءات الأمنية	فعالة	55.9
	مقبولة	41.9
	غير فعالة	2.2
مشاكل أمنية	نعم	2.2
	لا	97.8
رضاك عن جودة الخدمات	راضي جداً	32.3
	راضي	65.6
	غير راضي	2.2
ملاحظة التحديثات والتحسينات الدورية	نعم	52.7
	نادرًا	39.8
	لا	7.5
تلقي إشعارات كافية حول الطلب	نعم	93.5
	نادرًا	5.4

السؤال	الفئات	النسبة المئوية (%)
	لا	1.1
التوصية باستخدام التطبيق	نعم	91.4
	لا	8.6