

مخاطر خدمات الدفع الالكتروني وعلاقتها بحدوث الجرائم الالكترونية
(دراسة تطبيقية على قطاع خدمات المدفوعات بالمملكة العربية السعودية)

إعداد الطالبة:

ندى منصور بن داود

233001438

إشراف:

د. فايز علي جراد

د. الفيصل عبدالحميد محمد

العام الدراسي:

2024

**The Risks of Electronic Payment Services and Their Relationship
to Electronic Crimes
(Applied Study on the Payment Services Sector in the Kingdom of
Saudi Arabia)**

student preparation

Nada Mansour Bin Dawood

233001438

Supervisor:

Dr. Al-Faisal Abdul Hamid Muhammad

D. Fayez Ali Jarad

school year

2024

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

حقوق النشر

جميع الحقوق محفوظة للجامعة، ولا يسمح بنسخ هذه الرسالة أو ترجمتها إلى أي لغة من اللغات أو إعادة إصدارها أو أي جزء منها بأي شكل من الأشكال أو بأي وسيلة من الوسائل إلا بإذن خطي مُسبق من صاحب الرسالة أو القسم العلمي بالجامعة، مع لزوم الإشارة المرجعية لها عند الاقتباس منها، ويجب أن تكون هذه الصفحة جزءاً مع أي نُسخ إضافية.

المخلص

في ظل تنامي الاعتماد على التقنيات الحديثة واعتماد العديد من المؤسسات والأفراد على أنظمة الدفع الإلكتروني، ظهرت العديد من التهديدات الأمنية التي قد تؤدي إلى حدوث الجرائم الإلكترونية، ومن هنا هدفت الدراسة إلى التعرف على خدمات الدفع الإلكتروني، والمخاطر المرتبطة بها، ومعرفة العوامل التي تسهم في تقليل مخاطر خدمات الدفع الإلكتروني، والتطرق إلى نوع العلاقة بين هذه المخاطر وحوادث الجرائم الإلكترونية المرتبطة بها، تم استخدام المنهج الوصفي التحليلي، وتم الاعتماد على أداتين لتحقيق أهداف البحث وهما استبيان موجه للمستهلكين واستبيان موجه للعاملين في مجال خدمات الدفع الإلكتروني، وبلغت عينة الدراسة (80) مبحوث من العاملين و(162) من المستخدمين لخدمات الدفع الإلكتروني، حيث تم حساب التكرارات والنسب المئوية والمتوسط الحسابي والموزون والانحراف المعياري فضلاً عن معامل ارتباط بيرسون الفاكرونباخ، وتوصلت الدراسة إلى مجموعة نتائج من أبرزها:

- يرى العاملون في مجال خدمات الدفع الإلكتروني بأن العملاء يستخدمون خدمات الدفع بشكل يومي ومتكرر من أجل تسديد الفواتير والاشتراكات، كما أن هذه الخدمات تحمل مخاطر عالية تتعلق بالاختراقات الأمنية والاحتيال المالي، ومن أبرز العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني توعية العملاء وتشفير بيانات المستهلكين واستخدام البرامج المضادة للفيروسات، بالإضافة إلى أن أبرز التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم تتمثل في التحقق من هوية العميل واستخدام بروتوكول آمن بين المستخدم والمخدم المالي.

- يرى المستهلكون بأن خدمات الدفع الإلكتروني تستخدم من أجل تسديد الفواتير والاشتراكات ويتم ذلك عن طريق الهاتف المحمول والبطاقات الائتمانية، إلا أن هذه الخدمات تحمل مخاطر عالية تتعلق بالاختراقات الأمنية والاحتيال المالي، في حين تشفير بيانات المستهلكين وتجريم الأفعال التي فيها مساس بالأنظمة الإلكترونية يسهم في تقليل المخاطر، كما أن البنوك والمؤسسات المالية في المملكة تقدم مستوى عالٍ من الحماية فضلاً عن أن خدمات الدعم الفني المتاحة تساعد المستهلك على التعامل مع المشكلات الأمنية هذا من ناحية، ومن ناحية ثانية فضّل المستهلكون تلقي تنبيهات فورية عند استخدام حسابهم واستخدام خدمات دفع توفر تقنيات تحقق إضافية، بالإضافة إلى أن أبرز التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم تتمثل في التصريح الفوري حيال ضياع البطاقة واعتماد مواقع دفع آمنة واستخدام كلمات سر قوية.

Summary

The study aimed to identify electronic payment services in the Kingdom of Saudi Arabia, and the risks associated with electronic payment services, as well as clarifying the concept of electronic crimes and their types, knowing the factors that contribute to increasing or reducing the risks of electronic payment services and the extent of their impact on electronic crimes, and addressing the type of relationship between these The risks of payment services, the occurrence of electronic crimes associated with them, and the impact of the risks of electronic payment services on the level of security and trust among users of these systems in the Kingdom of Saudi Arabia. The descriptive analytical approach was used, Two tools were relied upon to achieve the research objectives. The study sample consisted of (80) employee respondents and (162) users of electronic payment services, where frequencies, percentages, weighted arithmetic mean, and standard deviation were calculated, as well as the Pearson-Cronbach correlation coefficient. The study reached a set of results, the most prominent of which are:

- Those working in the field of electronic payment services believe that customers use payment services on a daily and frequent basis in order to pay bills and subscriptions, and that these services carry high risks related to security breaches and financial fraud. Among the most prominent factors that contribute to reducing the risks of electronic payment services is customer awareness and data encryption. Consumers and the use of anti-virus programs, in addition to the most prominent measures that the organization can follow to reduce these risks and crimes are to verify the customer's identity and use a secure protocol between the user and the financial server.
- Consumers believe that electronic payment services are used to pay bills and subscriptions, and this is done via mobile phones and credit cards. However, these services carry high risks related to security breaches and financial fraud, while the study found that encrypting consumer data and criminalizing acts that compromise electronic systems It contributes to reducing risks, and banks and financial institutions in the Kingdom provide a high level of protection, in addition to the technical support services available that help the consumer deal with security problems. On the one hand, On the other hand, consumers preferred to receive immediate alerts when using their account and to use payment services that provide additional verification techniques. In addition, the most prominent measures that the organization can follow to reduce these risks and crimes are to immediately declare if the card is lost, adopt safe payment sites, and use strong passwords.

إهداء

إلى من كان لهم الفضل الأكبر في حياتي...

إلى أمي الغالية ، من علمتنا معنى الإصرار والصبر وغرست فينا حب العلم.
إلى زوجي ورفيق دربي ، الذي تحمل معي الصعاب وكان عوناً وسنداً لي لتحقيق هذا الإنجاز.
إلى أبنائي الأعزاء ، الذين كانوا مصدر إلهامي وقوتي .
إلى عائلتي الكريمة، الداعمين لي في كل خطوة.

إلى كل من آمن بي وبقدراتي ..

أهديكم هذا العمل، تعبيراً عن امتناني وحيي وتقديري.

شكر ونفك

الحمد لله الذي بنعمته تتم الصالحات.

أود أن أتقدم بجزيل الشكر وعظيم الامتنان لكل من ساهم في إنجاح هذا المشروع البحثي.

أولاً، أشكر الله عز وجل الذي منحني القوة والصبر لإتمام هذا البحث.

كما أتوجه بجزيل الشكر والتقدير لمشرف البحث وأعضاء لجنة التحكيم على وقتهم الثمين وملاحظاتهم البناءة التي ساهمت في تحسين هذا العمل.

كما لا يفوتني أن أشكر أسرتي وعائلتي الكريمة على دعمهم وتشجيعهم الدائم لي خلال فترة الدراسة، فلولا دعمهم لما تمكنت من تحقيق هذا الإنجاز.

والله ولي التوفيق.

فهرس الموضوعات

الصفحة	المحتويات
b	البسمة
c	حقوق النشر
d	الملخص
f	الإهداء
g	الشكر والتقدير
ن	مصطلحات الدراسة

الفصل الأول: الإطار العام للدراسة

2	- المقدمة
5	1. مشكلة الدراسة
6	2. أهمية الدراسة
7	3. أهداف الدراسة
7	4. تساؤلات الدراسة
8	5. فروض الدراسة
8	6. الدراسات السابقة
12	7. المنهجية وطرق البحث
13	8. حدود الدراسة

الفصل الثاني: الإطار النظري

- 16 أولاً- مدخل على خدمات الدفع بالمملكة العربية السعودية
- 16 1. مفهوم خدمات الدفع
- 17 2. أنواع خدمات الدفع
- 20 3. مزايا خدمات الدفع
- 21 4. مخاطر خدمات الدفع
- 28 5. العوامل التي تسهم في تقليل مخاطر خدمات الدفع
- 30 ثانياً- مدخل للجرائم الإلكترونية
- 30 1. مفهوم الجرائم الإلكترونية
- 31 2. أركان الجريمة الإلكترونية
- 32 3. خصائص الجريمة الإلكترونية
- 34 4. أنواع المجرمين في الجريمة الإلكترونية
- 34 5. أهداف الجرائم الإلكترونية
- 35 6. أنواع الجرائم الإلكترونية المرتبطة بخدمات الدفع الإلكتروني
- 39 ثالثاً- العلاقة بين مخاطر أنظمة الدفع الإلكتروني وحوادث الجرائم الإلكترونية.

الفصل الثالث: منهجية الدراسة

- 42 أولاً- منهج الدراسة
- 42 ثانياً- مجتمع وعينة الدراسة.
- 42 ثالثاً- خصائص أفراد الدراسة
- 47 رابعاً- أدوات الدراسة.
- 49 خامساً- صدق أدوات الدراسة.
- 53 سادساً- أساليب المعالجة الإحصائية.

الفصل الرابع: نتائج الدراسة

- تمهيد

- 56 أولاً- تحليل نتائج الاستبيان الموجه للعاملين
- 67 ثانياً- تحليل نتائج الاستبيان الموجه للمستهلكين

الفصل الخامس: مناقشة النتائج والتوصيات والخاتمة

- 79 أولاً- خلاصة الدراسة.
- 79 ثانياً- أهم نتائج الدراسة.
- 83 ثالثاً- توصيات الدراسة.
- 84 رابعاً- مقترحات الدراسة
- 85 قائمة المراجع
- 90 الملاحق

فهرس الجداول

الرقم	الموضوع	الصفحة
1	جدول رقم (3-1) يبين توزيع أفراد الدراسة وفق متغير المستوى التعليمي للعاملين	43
2	جدول رقم (3-2) يبين توزيع أفراد الدراسة وفق متغير المستوى التعليمي للمستهلكين	44
3	جدول رقم (3-3) يبين توزيع أفراد الدراسة وفق متغير التخصص المهني للمستهلكين	45
4	جدول رقم (3-4) يبين توزيع أفراد الدراسة وفق متغير عدد سنوات الخبرة للعاملين	46
5	جدول رقم (3-5) يبين محاور استبانة العاملين وعباراتها	47
6	جدول رقم (3-6) يبين محاور استبانة المستهلكين وعباراتها	48
7	جدول رقم (3-7) يبين تقسيم فئات مقياس ليكرت الخماسي (حدود متوسطات الاستجابة)	48
8	جدول رقم (3-8) يبين معاملات ارتباط بيرسون لعبارات المحاور مع الدرجة الكلية للمحور الخاصة باستبانة العاملين	49
9	جدول رقم (3-9) يبين معاملات ارتباط بيرسون للمحاور مع الدرجة الكلية للاستبانة الموجهة للعاملين	50
10	جدول رقم (3-10) يبين معاملات ارتباط بيرسون لعبارات المحاور مع الدرجة الكلية للمحور الخاصة باستبانة المستهلكين	51
11	جدول رقم (3-11) يبين ارتباط بيرسون للمحاور مع الدرجة الكلية للاستبانة الموجهة للعاملين	52
12	جدول رقم (3-12) معامل ألفا كرونباخ والتجزئة النصفية (Split-half) لقياس ثبات أدلة الدراسة الموجهة للعاملين	52

13	جدول رقم (3-13) معامل ألفا كرونباخ والتجزئة النصفية (Split-half) لقياس ثبات أداة الدراسة الموجهة للمستهلكين	53
14	جدول رقم (4-1) يبين استجابات أفراد الدراسة من العاملين حول خدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة	56
15	جدول رقم (4-2) يبين استجابات أفراد الدراسة من العاملين حول المخاطر المرتبطة بخدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة	58
16	جدول رقم (4-3) يبين استجابات أفراد الدراسة من العاملين حول العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة	60
17	جدول رقم (4-4) يبين استجابات أفراد الدراسة من العاملين حول العلاقة بين مخاطر الدفع الإلكتروني وحدوث الجرائم الإلكترونية في السوق السعودي مرتبة تنازلياً حسب متوسطات الموافقة	62
18	جدول رقم (4 - 5) استجابات أفراد الدراسة من العاملين حول التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم مرتبة تنازلياً حسب متوسطات الموافقة	64
19	جدول رقم (4 - 6) استجابات أفراد الدراسة من المستهلكين حول خدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة	67
20	جدول رقم (4 - 7) استجابات أفراد الدراسة من المستهلكين حول المخاطر المرتبطة بخدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة	69
21	جدول رقم (4 - 8) استجابات أفراد الدراسة من المستهلكين حول العوامل التي تساهم في تقليل مخاطر	70

	خدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة	
72	جدول رقم (4 - 9) استجابات أفراد الدراسة حول تأثير مخاطر الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة مرتبة تنازلياً حسب متوسطات الموافقة	22
74	جدول رقم (4 - 10) استجابات أفراد الدراسة من المستهلكين حول العلاقة بين مخاطر الدفع الإلكتروني وحدوث الجرائم الإلكترونية في السوق السعودي مرتبة تنازلياً حسب متوسطات الموافقة	23
76	جدول رقم (4 - 11) استجابات أفراد الدراسة من المستهلكين حول التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم مرتبة تنازلياً حسب متوسطات الموافقة	24

فهرس الأشكال

رقم الصفحة	اسم الشكل
43	شكل رقم (3-1) توزيع أفراد الدراسة من العاملين وفق متغير المستوى التعليمي
44	شكل رقم (3-2) توزيع أفراد الدراسة من المستهلكين وفق متغير المستوى التعليمي
45	شكل رقم (3-3) توزيع أفراد الدراسة من العاملين وفق متغير التخصص المهني.
46	شكل رقم (3-4) توزيع أفراد الدراسة من العاملين وفق متغير عدد سنوات الخبرة

مصطلحات الدراسة

- **خدمات الدفع الإلكتروني:** هي مجموعة الأدوات والوسائل والتقنيات الرقمية المتطورة، المستخدمة في مجال المعاملات المالية، وذلك بهدف تيسير إجراء التعاملات المصرفية بين العملاء والمؤسسة المالية، والتي تتضمن جميع التفاصيل المالية بين المؤسسات والأفراد.
- **مقدمي خدمات الدفع الإلكتروني:** وهم الجهات المسؤولة عن المعاملات النقدية، ومن أبرز هذه الجهات هم البنوك وشركات الصرافة والتحويل المالي عبر الإنترنت والحاصلين على ترخيص قانوني من البنك المركزي للعمل ضمن هذه الأنشطة.
- **الدفع الإلكتروني:** يقصد به عدد من الخدمات التي تقدمها الشركات المالية والمصرفية من أجل تيسير القيام بالتعاملات النقدية بطريقة آمنة وسهلة، وتتكون من البرامج والتقنيات والتطبيقات الخاصة بهذا المجال، كما تتصف هذه الخدمات بخضوعها لمجموعة من القوانين التي تحكمها، بشرط أن تتم هذه المعاملات بطريقة سرية، مع الحفاظ على أمان المستخدم وحمايته ضد أي تهديدات.
- **الجرائم الإلكترونية:** هي أنشطة غير مشروعة تنطلق من رغبة وإصرار مرتكبها، ومخالفة للقوانين والتشريعات (عبدالله، 2011، 53)، فهي أي فعل غير مشروع يتم من خلال استخدام نظام حاسوبي أو عبر شبكة الإنترنت.

Electronic Payment Services: A set of techniques and technological methods resulting from the technological revolution, introduced into the banking system to facilitate banking operations among various economic parties and general dealings. These services include all financial information between organizations, individuals, and companies.

Electronic Payment Service Providers: Banks, exchange companies, or electronic money transfer and payment companies licensed by the central bank to engage in any activities of managing and operating electronic payment systems or any of the payment services activities, including electronic money transfer activities.

Electronic Payment: An integrated system provided by financial and banking institutions to make the electronic payment process safe and convenient. This system usually consists of specific systems and programs and is characterized by being subject to a set of rules and regulations that ensure all financial transactions and procedures are conducted with complete confidentiality to guarantee user protection and security.

Cybercrime: An unlawful act resulting from a criminal intent for which the law prescribes a penalty (Abdullah, 2011, p. 53). It is any crime that can be committed using a computer system or computer network. This crime generally includes all crimes that can be committed in an electronic environment

الفصل الأول

الإطار العام للدراسة

- مقدمة

1. مشكلة الدراسة.
2. أهمية الدراسة.
3. أهداف الدراسة.
4. تساؤلات الدراسة.
5. فروض الدراسة.
6. الدراسات السابقة.
7. المنهجية وطرق البحث.
8. حدود الدراسة.
9. محددات الدراسة.

الفصل الأول

الإطار المنهجي للدراسة

مقدمة:

شهد العالم ثورة معلوماتية مذهلة في كافة قطاعات الحياة، ومن أبرز تلك القطاعات قطاع الاتصالات والأجهزة المتطورة، وفي ظل التطورات المستمرة التي رافقتها كان من أوجه انتفاضتها ظهور تطبيقات وأجهزة متطورة حديثة، ومن أبرزها اقتصاد المعرفة والتجارة الإلكترونية، كما بات استخدام هذه الأجهزة والتطبيقات رئيسياً في قطاع التجارة والصناعة (العجمي، 2014).

الأمر الذي نتج عنه حصول نمواً وازدهاراً واضحاً في مجال التجارة وبروز شكل جديد للتجارة، هي التجارة التي تتم عن طريق الإنترنت أو ما يعرف بالتجارة الإلكترونية، هذا الشكل ما زال يزداد تأثيره بشكل مستمر في الأسواق وفي الأداء الشرائي للأفراد، وساهم الإنترنت في نمو هذا النوع من التجارة في كل دول العالم، وعليه تنبعت جميع بلدان العالم إلى ضرورة اعتماد التجارة التي تتم عبر الإنترنت بسبب النتائج الإيجابية التي ترافقها، ومن أبرز هذه النتائج ارتفاع معدلات النمو والأرباح، فضلاً عن قدرتها على رفع معدل الروح التنافسية بين المنتجين، وذلك من خلال الترويج لمنتجاتهم وعرض جميع تفاصيلها، الأمر الذي أدى إلى تشجيع المستهلكين لطلبها واقتنائها بكل سهولة ويسر. وفي السياق نفسه نجد بأن جميع الدول اتجهت نحو وضع القواعد الأساسية لاعتماد التجارة التي تتم عن طريق الإنترنت وتأمين البنى التحتية المساعدة في نموها وتطورها وذلك بهدف التحول إلى اقتصاد رقمي يعتمد بشكل أساسي على الإنترنت (طالة، 2022).

وهنا لابد من الإشارة إلى التوجه العالمي نحو الرقمنة، ولاسيما في المجال المصرفي الذي صار يعتمد بدرجة أساسية على سرعة إجراء التبادلات المالية عن طريق الإنترنت، هذه التعاملات تشمل على تحويل مبالغ مالية كبيرة من خلال الدفع الإلكتروني، ولما كان الفاعلون في إدارة هذا المجال، حريصون على إيجاد نظام عالمي موحد يواكب الاتجاهات الدولية لتطوير الصيرفة الإلكترونية العالمية، التي شهدت قفزة نوعية في الآونة الأخيرة، وذلك بسبب تسارع المعاملات التجارية والنقدية ومع اقترانها مع الظروف

الصحية المتعلقة بفيروس كورونا، مما استدعى إلى ضرورة تطويرها وإيجاد نوع بديل للصيرفة الكلاسيكية، المعروف عنها بطء إجراءاتها وروتينها البيروقراطي إلى عالم رقمنة معاصر والتي من شأنه أن يوفر على المصرف وعلى الزبون مشكلة التواجد الشخصي لدى المصارف، بنظام لا يؤمن بالمواعيد والمواقيت الخاصة بفتح المصارف وغلقتها، ولا يحتاج لتواجد المستهلك أمام صراف آلي أو شباك مصرف بل يقتصر الأمر على معلومات رقمية تحتوي على معلومات دقيقة تخص العميل الذي بإمكانه القيام بالتبادلات التجارية من بيع وشراء وتحويلات مالية وغيرها في أي وقت شاء وبسرعة وهو جالس في بيته دون عناء التقل أو تكليف أو إصدار أوامر بالوكالة، مشمولاً بجملة من الإجراءات والضمانات بسرية (سمير، 2021)

"ونتيجة لهذه التطورات، كان لابد للمؤسسات المصرفية والمالية من استثمار تكنولوجيا المعلومات والاتصال، وشبكة الإنترنت لتقديم خدماتها إلى العملاء، من خلال إيجاد نوع من الحسابات الإلكترونية، وتوفير أدوات ووسائل دفع إلكترونية لتسوية المعاملات التي تكفل نقل الحقوق والديون من حساب إلى آخر أو من شخص إلى آخر بطريقة الكترونية وهو ما يطلق عليه بنظام الدفع الإلكتروني، والذي يتيح لعملاء المصارف والبنوك من إجراء بعض العمليات المصرفية الإلكترونية، كعمليات البيع والشراء وتحويل الأموال والتي تتم من خلال شبكة الإنترنت عن طريق استعمال وسائل وأدوات الدفع الإلكتروني كبطاقات الدفع الإلكترونية سواء الائتمانية منها أو بطاقات الوفاء، والنقود الإلكترونية وغيرها" (الفليح، 2021، 1)

وفي ظل التطور المستمر والاستخدام الكبير للتقنيات الحديثة، تبرز المملكة العربية السعودية كسوق مزدهر ومتطور للاعتماد على التجارة التي تتم عن طريق الإنترنت. مع تزايد عدد المستخدمين الذين يعتمدون على الإنترنت لكل شيء، من الشراء اليومي إلى الاستثمارات الكبيرة، مما يعكس الديناميكية الاقتصادية المتنوعة للسعودية. هذا التوسع لم يكن ليحدث دون التطور اللافت لنظم حلول الدفع الإلكتروني بالسعودية، التي شغلت دوراً بارزاً في نمو وتيرة التحول الرقمي في البلاد.

ونظراً لتنوع تطبيقات عملية الدفع الإلكتروني أدى ذلك إلى ظهور عدد من المخاطر في عمليات الدفع الإلكتروني والتي فرضت على الدول ضرورة اللحاق بهذه التطورات من خلال وضع أسس أمنية تحكم نظم التجارة التي تتم عن طريق الإنترنت، وذلك سعياً لتأمين التبادلات المادية للأفراد والمتعاملين

من الآثار السلبية لهذه التجارة. حيث أن معاملات الدفع الإلكتروني تحمل عدد من المخاطر وفي بعض الأحيان تستخدم لإحداث الضرر في الأفراد، والقيام بأشكال متنوعة من الإجرام الناعم (لعماري، 2019). وعلى الرغم من الصعود السريع لقطاع التجارة التي تتم عن طريق الإنترنت، إلا أنه يواجه مجموعة من التحديات المتأصلة في عالمها الرقمي. فلقد وفرت سرعة المعاملات الرقمية المجال لانتشار أنشطة غير مشروعة، تتنوع هذه الأنشطة من مشكلة غسل الأموال إلى حدوث الهجمات السيبرانية، حيث تعد هذه الأنشطة من التحديات التي تهدد سلامة النظام المالي مما يتطلب جهود تنظيمية يقظة واتخاذ تدابير وقائية قوية (حمزة، 2024).

وهذا " الإجرام المستحدث " قد انتشر مع تطور نمو التجارة التي تتم عن طريق الإنترنت، ومن الجدير بالذكر إلى أن العمليات غير المشروعة التي تجري عن طريق التكنولوجيا تصنف على أنها جريمة إلكترونية، وهنا ينبغي القول إلى الجريمة الإلكترونية هي عبارة عن ومضات كهربائية ومغناطيسية، ورموز، وشفرات، كما اهتم المجتمع الدولي بإقرار اتفاقات دولية لوضع قوانين موحدة تخضع لها جميع الدول، وتقوم المملكة العربية السعودية بفرض تشريعات صارمة لمحاسبة المخالفين والذين يقومون بفعل الاجرام الالكتروني وملاحقتهم ومعاقبتهم (سفر، 2008).

وبناء على ما سبق نجد أن المملكة العربية السعودية تعمل على تهيئة بيئة آمنة لأفراد شعبها وأيضاً المقيمين فيها، ومع الاعتماد على التجارة التي تتم عن طريق الإنترنت، زادت الجرائم الإلكترونية، ومع كثرة هذه الجرائم يتضح لنا مقدار الجهود التي تبذلها المملكة للحد من تزايد هذه الجرائم للوصول لغايتها في بناء مجتمع سعودي آمن يخلو من هذه الجرائم.

لذا خلال هذه الدراسة سيتم التطرق إلى مخاطر أنظمة الدفع الإلكتروني وعلاقتها بحدوث الجرائم الإلكترونية، وهنا ينبغي القول إلى أنه تم اختيار السوق السعودي كمجال للدراسة، وذلك بسبب التطور الكبير في استخدام التقنيات الرقمية وزيادة الاعتماد على أنظمة الدفع الإلكتروني في الفترة الأخيرة، وذلك في إطار الرؤية الإستراتيجية للبنك المركزي السعودي المعتمدة على مستهدفات برنامج تطوير القطاع المالي، الهادف إلى تعزيز الدفع الإلكتروني، وخفض كميات التعاملات النقدية وذلك من أجل الوصول بكمية المدفوعات الإلكترونية إلى نسبة تصل لـ 70% من إجمالي عمليات الدفع مع بداية عام 2025م.

1. مشكلة الدراسة:

أدى التطور التكنولوجي إلى ازدهار التجارة التي تتم عن طريق الإنترنت في جميع الدول، إلا أن الاعتماد على هذا النموذج من التجارة ساهم في ظهور عدد من التحديات المواقبة لتطبيقها، ومن أبرزها المخاطر المرتبطة بأنظمة الدفع الإلكتروني الذي يمس مختلف جوانب معاملات الدفع الإلكتروني لحماية المتعاملين، الأمر الذي فرض على الدول اللحاق بها من خلال وضع أساس قانوني ينظم هذا النوع من التجارة للتعامل مع الإشكالات التشريعية المرافقة لها والتي لابد من مواجهتها بشكل صحيح وفعال للحد من تزايد وقوع هذا النوع من الجرائم، ويرتبط مباشرة بالجرائم المستحدثة المتعلقة بمخاطر أنظمة الدفع. فالجانب القانوني هو الأساس للحد من تزايد وقوع هذه الجرائم ويساعد في الوقت نفسه على ازدهار معاملات التجارة الإلكترونية واستمرارها (ذهيبة، 2018).

وفي ظل تنامي الاعتماد على التقنيات الحديثة واعتماد العديد من المؤسسات والأفراد على أنظمة الدفع الإلكتروني، ظهرت العديد من التهديدات الأمنية التي قد تؤدي إلى حدوث الجرائم الإلكترونية. وهنا تجدر الإشارة إلى أن الأسواق السعودية تشهد نمواً ملحوظاً في استخدام خدمات الدفع الإلكتروني، مما يجعلها عرضة لهذه المخاطر بشكل أكبر. تتمثل مشكلة هذا البحث في فهم العلاقة بين مخاطر أنظمة الدفع الإلكتروني وحوادث الجرائم الإلكترونية، وكيفية تأثير هذه المخاطر على مستوى الأمان والثقة لدى المستخدمين.

وهنا تتجلى مشكلة الدراسة من خلال التساؤل التالي:

"ما هي العلاقة بين مخاطر أنظمة الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي؟ وكيف يمكن أن تؤثر هذه المخاطر على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة؟"

2. أهمية الدراسة:

تتجلى من الدور الهام الذي تشغله أنظمة الدفع الإلكتروني من خلال سرعة التبادلات النقدية وتعزيز نمو الاقتصاد الرقمي في المملكة. ومع تزايد استمال هذه الأنظمة، أصبح من الضروري فهم المخاطر والتحديات المتعلقة بها وتأثيرها على الأمن السيبراني وحوادث الجرائم الإلكترونية، لذلك تتضح أهمية هذه الدراسة من كونها تحاول تحقيق الآتي:

- تساهم الدراسة في تحديد وتحليل أنواع المخاطر التي ترافق تزايد الاعتماد على أنظمة الدفع الإلكتروني، مما يساعد في رفع مستوى الوعي الأمني بين العملاء والشركات.
- من خلال فهم العلاقة بين مخاطر أنظمة الدفع الإلكتروني وحوادث الجرائم الإلكترونية، يمكن تقديم توصيات فعالة لتحسين الإجراءات الأمنية وتقليل فرص الاختراقات والجرائم الإلكترونية.
- تساهم نتائج الدراسة في توفير معلومات قيمة لصناع القرار والشركات المتخصصة في إيجاد أنواع متطورة من أنظمة الدفع الإلكتروني، لرفع مستوى الأمان وتساهم في الوقت نفسه في زيادة ثقة المستخدمين.
- تحاول الدراسة توضيح التحديات الأمنية المرتبطة بأنظمة الدفع الإلكتروني، مما قد يدفع الشركات إلى ابتكار حلول وتقنيات جديدة لتعزيز أمان هذه الأنظمة.
- تضاف الدراسة إلى مجموعة الأدبيات الأكاديمية المتعلقة بأمن أنظمة الدفع الإلكتروني والجرائم الإلكترونية، مما يساهم في فتح مجالات جديدة للبحث العلمي الأكاديمي.

فتمثل الأهمية العلمية للدراسة: في تناول موضوع مهم يمس مصالح فئة كبيرة من المتعاملين بشكل مستمر في التجارة التي تتم عن طريق الإنترنت، وذلك من خلال الكشف عن المخاطر والتحديات المهددة لأنظمة الدفع الإلكتروني وشرح الأنماط المستجدة من الجرائم الإلكترونية.

أما الأهمية العملية للدراسة: فتمثل في محاولة إيجاد حلول للمشكلات والمخاطر المتعلقة بأنظمة الدفع الإلكتروني في السوق السعودي تفيد الجهات المعنية لمنع وقوع جرائم إلكترونية تتم عن طريق الدفع الإلكتروني. وأيضاً يمكن للباحثين والمهتمين في مجال الدراسة الاستفادة من توصياتها وتطويرها لإجراء دراسات معمقة في أحد أهم مجالات التقنيات المتطورة والتي ترتبط بمجال تنمية الاقتصاد الرقمي.

3. أهداف الدراسة:

- التعرف على خدمات الدفع الإلكتروني في المملكة العربية السعودية.
- التعرف على المخاطر المرتبطة بخدمات الدفع الإلكتروني .
- التعرف على مفهوم الجرائم الإلكترونية وأنواعها .
- التعرف على العوامل التي تسهم في زيادة أو تقليل مخاطر خدمات الدفع الإلكتروني ومدى تأثيرها على الجرائم الإلكترونية.
- التعرف على العلاقة بين هذه مخاطر خدمات الدفع وحوادث الجرائم الإلكترونية المرتبطة بها.
- التعرف على تأثير مخاطر خدمات الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة في المملكة العربية السعودية.
- تقديم التوصيات والحلول للمؤسسات والشركات العاملة في قطاع خدمات المدفوعات لتعزيز الأمان الإلكتروني والحد من الجرائم الإلكترونية.

4. تساؤلات الدراسة :

- ١ . ما هي خدمات الدفع الإلكتروني؟
- ٢ . ما هي المخاطر المرتبطة بخدمات الدفع الإلكتروني؟
- ٣ . ما هي العوامل التي تسهم في زيادة أو تقليل مخاطر خدمات الدفع الإلكتروني؟
- ٤ . ماهي الجرائم الإلكترونية؟
- ٥ . ما هو تأثير مخاطر خدمات الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة؟
- ٦ . ما هي العلاقة بين مخاطر أنظمة الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي؟
- ٧ . ماهي التدابير التي يمكن اتخاذها للحد من هذه المخاطر والجرائم؟

5. فروض الدراسة:

- تختلف المخاطر المرتبطة بخدمات الدفع الإلكترونية بناءً على نوع الخدمة المقدمة (مثل الدفع عبر الهاتف المحمول، الدفع عبر الإنترنت، إلخ).
- يوجد أثر لمخاطر خدمات الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة.
- يفترض وجود علاقة بين مخاطر خدمات الدفع الإلكتروني وحوادث الجرائم الإلكترونية .
- يفترض أن وجود ثغرات في أنظمة الأمان لخدمات الدفع الإلكتروني في السوق السعودي يزيد من احتمالية حدوث جرائم إلكترونية
- يوجد أثر لاستخدام التقنيات الحديثة في خدمات الدفع الإلكترونية على مستوى الأمان والسيطرة على الجرائم المالية في شركات المدفوعات السعودية.
- يوجد أثر لوجود تشريعات قوية وفعالة للأمان السيبراني في المملكة العربية السعودية على تقليل معدلات الجرائم الإلكترونية المتعلقة بخدمات الدفع الإلكتروني.

6. الدراسات السابقة:

أولاً الدراسات العربية:

الدراسة الأولى: الجهيمي، عبدالرحمن و د. أحمد، شهاب (2023). الخدمات الإلكترونية وأثرها على المستهلكين في المملكة العربية السعودية. دراسة ميدانية. المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، مصر، 4 (13)، 101 – 120

هدفت هذه الدراسة للتعرف على مستوى مصداقية وسهولة الخدمات التي تتم عن طريق الإنترنت المقدمة من المنشآت السعودية للمستهلكين، وذلك عن طريق فهم النتائج الإيجابية للخدمات التي تتم عن طريق الإنترنت على المستهلكين، كما تناولت هذه الدراسة عدة جوانب متنوعة للتعامل بين العملاء والخدمات الإلكترونية التي يكونون بحاجة إليها، فضلاً عن تقييم مدى رضا المستهلكين عن تلك الخدمات

وتحليل جودتها ومدى أمانها، وتحديد أبرز المشكلات التي تواجه العملاء عند تعاملهم مع هذه الخدمات، واقتراح فرص للتحسين في تقديم تلك الخدمات لجعلها أكثر فعالية وأماناً.

كما تتضمن الدراسة استعراضاً للإطار القانوني والتنظيمي الذي يحكم هذه الخدمات في المملكة، بهدف إعطاء مقترحات لتحسين هذا الإطار بما يتلاءم مع تطلعات المستهلكين.

الدراسة الثانية: خريسات، مي (2022). إيجابيات وسلبيات الدفع الإلكتروني في المؤسسات الحكومية. المجلة العربية للنشر العلمي. العدد واحد وأربعون .

هدفت هذه الدراسة لتقييم دور أنظمة الدفع الإلكتروني في المؤسسات الحكومية. وقد قامت بتوضيح أنواع أنظمة الدفع الإلكتروني المستخدمة عند إجراء الأنشطة المادية، وتقييم دور هذه الأنظمة في أنشطة التوفير، وتحديد النتائج الإيجابية والسلبية لاستخدام أنظمة الدفع الإلكتروني.

الدراسة الثالثة: د. طالة، لامية (2022). النقود الإلكترونية: بين تسهيل أنظمة الدفع الإلكتروني ومخاطرها على أمن المعاملات التجارية. مجلة الاستاذ الباحث للدراسات القانونية والسياسية -المجلد 66 - العدد 61 - جوان 26.

تهدف الدراسة إلى تقديم رؤية شاملة حول ماهية النقود الإلكترونية وتأثيرها على نظام الدفع الإلكتروني والأمن التجاري، مع تقديم توصيات لتعزيز الأمان والثقة في هذه التعاملات. كما تطرقت إلى توضيح دور هذه النقود في تسهيل عمل أنظمة الدفع وجعلها أكثر سرعة وكفاءة وسهولة للمستخدمين، بالإضافة إلى شرح التحديات القانونية المتعلقة باستخدام النقود الرقمية، مثل الاحتيال وسرقة البيانات والاختراقات الإلكترونية، ومن ثم حاولت تفسير كيفية تحقيق توازن بين فوائد استعمال تلك النقود والمخاطر المحتملة الناشئة عن استخدامها، واستعرضت القوانين واللوائح المرتبطة باستعمال هذه النقود، وقدمت توصيات لتحسين هذا الإطار بهدف الحد من تلك الأضرار وتعزيز الأمان عند التعامل مع خدمات الدفع الإلكتروني.

الدراسة الرابعة: الفليح، فلاح (2021). المسؤولية المدنية لمزود خدمات الدفع الإلكتروني. جامعة الشرق الأوسط.

تهدف هذه الدراسة إلى بحث وتوضيح الجوانب القانونية المرتبطة بمسؤولية مقدمي خدمات الدفع الإلكتروني، وتتناول الدراسة الأطر القانونية المحددة لعمل هؤلاء المزودين، والمسؤوليات الواقعة على

عانتهم تجاه العملاء في حال وقوع أي خلل أو عدم مسؤولية في تقديم الخدمات. كما تستعرض الدراسة كيفية حماية حقوق المستهلكين وضمان أمن تلك التفاعلات، فضلاً عن تقديم توصيات لتطوير القوانين المتعلقة بخدمات الدفع الإلكتروني.

الدراسة الخامسة: سمير، سبيحي (2021). مخاطر الدفع الإلكتروني . جامعة لونيبي علي البلدية – الجزائر. مجلة البحوث والدراسات القانونية والسياسية. السنة 12 المجلد 11 / العدد 02

هدفت إلى كشف وتوضيح المخاطر المتعلقة باستخدام أنظمة الدفع الإلكتروني. ركزت الدراسة على التحديات الأمنية التي يتعرض لها العملاء مثل الاحتيال، القرصنة، وسرقة المعلومات الشخصية. وتستعرض الدراسة الآثار السلبية لهذه التهديدات على المستخدمين والشركات المالية. من خلال هذا التحليل، كما تهدف الدراسة الوصول إلى توصيات لتحقيق الأمان عند إجراء عمليات الدفع الإلكتروني، مع وضع إجراءات وقائية للحد من هذه المخاطر.

الدراسة السادسة: د. لعماري، بوليد (2019). الضمانات القانونية ضد مخاطر استخدام وسائل الدفع الإلكتروني، كلية الحقوق. جامعة الجزائر

هدفت إلى تحليل وفهم المخاطر المتعلقة باستخدام وسائل الدفع الإلكتروني وتقديم ضمانات قانونية لمواجهة هذه المخاطر. حيث ركزت على تقييم الأضرار التي يمكن أن يتعرض لها العملاء عند استعمالهم لوسائل الدفع الإلكتروني واستعرضت وصف القوانين المحلية والعالمية المنظمة لاستخدام وسائل الدفع الإلكتروني ، وقدمت توصيات لضمانات قانونية وتدابير وقائية يمكن اتخاذها لحماية المستخدمين والتصدي للمخاطر المحتملة ، تهدف الدراسة في النهاية إلى تحسين الإطار القانوني الحالي وتعزيز الثقة في استخدام وسائل الدفع الإلكتروني من خلال توفير حصانة قانونية للعملاء .

الدراسة السابعة: ذهيبه، محمد (2018). مخاطر الدفع الإلكتروني عبر الإنترنت التي يتعرض لها المستهلك الإلكتروني وإستراتيجية الجزائر لحمايته: مشروع التصديق والتوقيع الإلكترونيين.

تهدف هذه الدراسة لتسلط الضوء على مخاطر الدفع الإلكتروني عبر الإنترنت التي من الممكن أن تواجه المستخدم، وتم تحديد دولة الجزائر كمجال مكاني للدراسة. كما تطرقت إلى كيفية استخدام البطاقات الائتمانية وإجراء التحويل المالي عن طريق الإنترنت، وشدد الباحث على أهمية وضع استراتيجية دقيقة للحد من التهديدات والمخاطر التي يتعرض لها العميل الإلكتروني.

الدراسة الثامنة: العجمي، عبدالله (2014). المشكلات العملية والقانونية للجرائم الإلكترونية. دراسة مقارنة. جامعة الشرق الأوسط.

هدفت إلى شرح مفهوم الجريمة التي تتم عن طريق الإنترنت، ومجموعة التهديدات التي تترافق مع حدوثها، وهدفت إلى السعي للتوصل إلى مجموعة حلول تطبيقية وقانونية لمواجهة الجرائم الإلكترونية، مع إجراء دراسة متعمقة عن كيفية مجابتهها عن طريق التطرق إلى مجموعة تشريعات دولية، ومن أبرزها هي التشريع الكويتي والأردني، حيث تطرقت إلى وصف التهديدات التي تواجهها الجهات المختصة في الحد من هذا النوع من الجرائم، وتوضيح نقاط الضعف القانونية في القوانين الحالية التي تعرقل الحد من انتشار هذه الجرائم الإلكترونية بفعالية بالإضافة إلى إجراء مقارنة للقوانين المرتبطة بالجرائم الإلكترونية في مختلف الدول، مع تحديد نقاط الاختلاف في كل منها، و قدمت توصيات لتعزيز الإطار القانوني وتحسين الإجراءات العملية لمواجهة تلك الجرائم.

الدراسة التاسعة: سفر، أحمد (2008). أنظمة الدفع الإلكتروني. منشورات الحلبي الحقوقية. لبنان.

قامت بتحليل نتائج أنشطة الدفع الإلكتروني على الأنشطة الحكومية. كما تتناول الدراسة الفوائد مثل تحسين الكفاءة والشفافية وسرعة إنجاز المعاملات، وكذلك التحديات مثل قضايا الأمان، والخصوصية، والاعتماد على التكنولوجيا، وتقديم توصيات لتحسين وتطوير نماذج الدفع الإلكتروني في المنظمات الحكومية.

الدراسة العاشرة: بركات، عزت (2000) . ظاهرة غسل الأموال وآثارها الاقتصادية والاجتماعية . جامعة الزرقاء الأهلية ، الأردن

تتناول الدراسة كيفية حدوث غسل الأموال وأساليبه المختلفة، بالإضافة إلى نتائجه السيئة مثل تشويه الأسواق المالية، تقويض الاقتصاد الشرعي، وزيادة الجريمة المنظمة. كما تركز الدراسة على الآثار الاجتماعية المتمثلة في الفساد وضعف الأمان غد التعامل مع المنظمات المالية. ومن خلال ذلك، تسعى الدراسة إلى تقديم توصيات للحد من هذه الظاهرة وتعزيز النظام المالي.

ثانياً: الدراسات الأجنبية:

1. Alyabes , Alhanoof – Alsalloum , Othman (2018) . Factors Affecting Consumers' Perception of Electronic Payment in Saudi Arabia . King Saud University.

هدفت هذه الدراسة إلى تقديم توصيات لتحسين خدمات الدفع الإلكتروني من خلال فهم العوامل المؤثرة على تصورات المستهلكين، مما يساعد على تعزيز استخدام هذه الخدمات بأمان وفعالية في المملكة العربية السعودية، كما وضحت مدى تأثير مستوى الثقة والأمان في الخدمات الإلكترونية على قرارات المستهلكين باستخدامها، وتحليل تأثير وعي المستهلكين ومعرفتهم بآليات وأمان الدفع الإلكتروني على تبنيهم لهذه الخدمات ودراسة تأثير سهولة استخدام خدمات الدفع الإلكتروني على قبول المستهلكين لها. وتقييم تأثير التجارب السابقة للمستهلكين مع خدمات الدفع الإلكتروني على تصوراتهم الآتية.

7. المنهجية وطرق البحث:

تم الاعتماد على المناهج الآتية:

- المنهج الوصفي التحليلي: وذلك من خلال وصف وتحليل المخاطر والتحديات والجرائم الإلكترونية المرتبطة بخدمات الدفع الإلكتروني.
- المنهج التطبيقي: لتطبيق النتائج على قطاع خدمات المدفوعات في المملكة

• عينة الدراسة:

تمثلت بالعاملين في مجال المدفوعات الإلكترونية والمستخدمين.

• طرق البحث :

تم الحصول على البيانات المطلوبة من خلال مصادر:

- أولية: عن طريق وضع استبيانات متخصصة لجمع بيانات من العاملين والمستهلكين.

- ثانوية: عن طريق الاعتماد على المراجع والأدبيات ذات الصلة، والاطلاع على القوانين واللوائح المتعلقة بخدمات الدفع الإلكتروني .

تم تحليل البيانات:

بطريقة كمية: باستخدام برنامج (SPSS)

بطريقة نوعية: باستخدام منهجية التحليل الموضوعي مما يساعد في فهم أعمق للمخاطر والجرائم الإلكترونية المتعلقة بخدمات الدفع الإلكتروني ومعرفة التحديات القائمة.

• أدوات الدراسة:

تم تصميم هذا البحث كدراسة حالة تطبيقية تعتمد على تحليل نوعي وكمي للبيانات، ولإجراء هذه الدراسة التطبيقية على مخاطر خدمات الدفع الإلكتروني وعلاقتها بحدوث الجرائم الإلكترونية في قطاع خدمات المدفوعات، ومن هذه الأدوات :

1. تصميم استبيانات موجهة للعاملين في قطاع المدفوعات الإلكترونية واستبيانات للمستخدمين النهائيين (المستهلكين) لجمع بيانات حول تجربتهم ووعيهم بالمخاطر.
2. الرجوع إلى الدراسات والأبحاث السابقة المرتبطة بالموضوع المدروس، وإلى أبرز المخاطر المتعلقة بالدفع الإلكتروني والتي تؤدي إلى وقوع الجرائم الإلكترونية.

8. حدود الدراسة :

- الزمانية:

اقتصرت على فترة زمنية محددة تبدأ من يناير 2020 حتى ديسمبر 2023. تم اختيار هذه الفترة لأنها شهدت تطوراً كبيراً في استخدام أنظمة الدفع الإلكتروني وخصوصاً بعد جائحة كورونا.

- المكانية:

السوق السعودي.

- الموضوعية :

- ١ . تحديد أنواع المخاطر التي تتعرض لها خدمات الدفع الإلكتروني، مثل مخاطر الأمان السيبراني، الاختراقات، التزوير، وسرقة البيانات الشخصية.
- ٢ . دراسة الجرائم المتعلقة بخدمات الدفع الإلكتروني.
- ٣ . تحليل كيف تؤدي المخاطر المحددة إلى حدوث الجرائم الإلكترونية من خلال الدراسة التطبيقية وتحليل البيانات .
- ٤ . استعراض الإجراءات الكفيلة بمواجهة هذه المخاطر والجرائم، بما في ذلك القوانين والتدابير التقنية.

9.محددات الدراسة

عدم وجود أي مانع من نشر النتائج التي تم التوصل إليها على المجتمع الأكاديمي والعلمي.

الفصل الثاني

الإطار النظري

أولاً- مدخل على خدمات الدفع بالمملكة العربية السعودية

1. مفهوم خدمات الدفع.
2. أنواع خدمات الدفع.
3. مزايا خدمات الدفع.
4. مخاطر خدمات الدفع.
5. العوامل التي تسهم في تقليل مخاطر خدمات الدفع.

ثانياً : مدخل للجرائم الإلكترونية

١. مفهوم الجرائم الإلكترونية
٢. أركان الجريمة الإلكترونية
3. خصائص الجريمة الإلكترونية
4. أنواع المجرمين في الجريمة الإلكترونية
5. أهداف الجرائم الإلكترونية
6. أنواع الجرائم الإلكترونية المرتبطة بخدمات الدفع الإلكتروني

ثالثاً : العلاقة بين مخاطر أنظمة الدفع الإلكتروني وحدوث الجرائم الإلكترونية

أولاً- مدخل على خدمات الدفع بالمملكة العربية السعودية:

1. مفهوم خدمات الدفع.

بسبب التطور التقني في نطاق أنظمة الدفع الإلكتروني المتعلقة بالبنوك فقد برزت وسائل وأدوات للدفع الإلكتروني تقوم على لمشاركة بالوسائل الرقمية للمعلومات البنكية لإرسال قيم النقود المتفق عليها من رصيد المدين إلى رصيد الدائن إن كان ضمن نفس المؤسسة الخاصة بالمدفوعات أو في مؤسسة أخرى بواسطة التحديث الرقمي المتعلق بوسائل الاتصال بمختلف أنواعها، فاتجهت المصارف إلى اعتماد هذه التقنيات التكنولوجية في صرف قيمة المستحقات وذلك عن طريق إدخال البيانات المتعلقة بالحسابات في أجهزة الحاسوب، واستخدام طريقة المقايضة، وتبادل النقود باستخدام التقنيات الرقمية بين البنوك، وبذلك أتاحت التكنولوجيا طرق تبادل حقيقية للنقود وهو ما يسمى بالدفع الإلكتروني، فأصبح الدفع الإلكتروني من أهم الخدمات المتوفرة لدى البنوك لعملائها إذ تمكنهم من شراء احتياجاتهم من السلع والخدمات، إضافة إلى تمكينهم من سحب مبالغ نقدية أو تحويلها وفق منظومة متكاملة (رضا، 2023).

البنك المركزي في كثير من الدول يعرف الدفع الإلكتروني على أنه استخدام الأنظمة والتقنيات الإلكترونية لتحويل الأموال بين الأفراد أو المؤسسات، وذلك بوسائل متعددة مثل بطاقات الائتمان، بطاقات الخصم، التحويلات البنكية الإلكترونية، والمحافظ الإلكترونية. الدفع الإلكتروني يتيح تنفيذ العمليات المالية بسرعة وفعالية عالية، ويوفر سجلات دقيقة للمعاملات، ويساهم في تعزيز الشفافية والحد من الجرائم المالية .

كما ويعرف التسديد باستخدام أنظمة الدفع الرقمية بأنه استخدام الأدوات والتقنيات الإلكترونية لإجراء المدفوعات وتحويل الأموال بطرق آمنة وسريعة، بدلاً من استخدام النقد التقليدي أو الشيكات الورقية، مما يعزز الكفاءة والشفافية في العمليات المالية.

ومن هنا نجد أن وسائل الدفع الإلكتروني هي قيم نقدية مخزنة إلكترونياً على النظام الإلكتروني لمؤسسة مالية معتمدة ومرخصة وتكون مقبولة كأداة دفع ووفاء للغير بناء على الاستراتيجية التي يستخدمها عميل مؤسسة خدمات المدفوعات (الشبول، 2023).

ومن أبرز خصائص خدمات الدفع الإلكتروني التي تجعلها خياراً جذاباً وفعالاً للعديد من المستخدمين والأعمال، مما يساهم في تطور الاقتصاد الرقمي وتحسين التجربة المالية بشكل عام:

- خدمات الدفع الإلكتروني طريقة رقمية مميزة ذات طابع دولي، أي أنه وسيلة مقبولة في كل دول العالم، حيث يستعمل نظام التسديد الرقمي لتسهيل إجراءات عرض وشراء البضائع من خلال الإنترنت، أي أن الاتفاق يتم بين الجانبين الذين تفصلهما مسافات بعيدة ويكون التسديد عن طريق الوسائط الرقمية (بريكة، 2014).
- عمليات الدفع الإلكتروني تتم بسرعة كبيرة، مما يوفر الوقت ويزيد من كفاءة المعاملات المالية مقارنة بالطرق التقليدية مثل الشيكات أو الدفع النقدي.
- يمكن إجراء المدفوعات في أي وقت ومن أي مكان باستخدام الإنترنت أو الهواتف الذكية، مما يوفر راحة كبيرة للمستخدمين.
- توفر خدمات الدفع الإلكتروني سجلات دقيقة للمعاملات، مما يسهل التتبع والمراجعة ويساهم في الشفافية المالية.
- يمكن دمج خدمات الدفع الإلكتروني بسهولة مع أنظمة المحاسبة والإدارة المالية الأخرى، مما يسهل إدارة الأعمال والعمليات المالية.
- توفر مجموعة متنوعة من الوسائل والأدوات مثل بطاقات الائتمان، المحافظ الإلكترونية، والتحويلات البنكية، مما يتيح للمستخدمين اختيار الوسيلة الأنسب لهم.
- في بعض الحالات، يمكن أن تكون رسوم خدمات الدفع الإلكتروني أقل من تكاليف المعاملات المالية التقليدية، مما يوفر تكلفة للمستخدمين والمؤسسات.

2. أنواع خدمات الدفع.

تميزت خدمات الدفع الإلكتروني باختلافها وتنوعها تبعاً لطبيعة العملية التي يحتاجها العميل، مما تتطلب أهمية كبيرة لوجود وسائل تستخدم للدفع الإلكتروني وذلك لتحقيق هدف استراتيجية البيع وتسويق المنتجات رقمياً ومن أبرز تلك الوسائل (بلطرش وآخرون، 2017):

أ. **بطاقة الائتمان:** وهي التي تعتمد عليها مؤسسات خدمات المدفوعات للزبائن بمساهمة من مؤسسات التسديد الموجودة في جميع الدول، حيث يستطيع حامل البطاقة استخدامها في إجراء عمليات سحب نقدي أو لدفع مشترياته من الأسواق التي تقبل التعامل عن طريقها ومن ثم تسديد قيمتها لاحقاً (قرومي، مرجع سابق، ص144).

ب. **النقود الإلكترونية:** وتسمى أيضاً الرقمية، وهي عبارة عن أموال ذات طابع محسوس تكون على شكل بيانات رقمية تحفظ ضمن موضع موثوق فيه على وسائط التخزين الثانوية المتعلقة بالزبون ويطلق عليها الحافظة الرقمية، إذ يمكن للعميل اعتماد الحافظة الرقمية في إتمام كل ما يتعلق بأمور العرض أو الطلب أو التحويل بدون أي تكلفة مالية، وعليه يتم استبدال العملات والأوراق النقدية بملفات موقعة رقمياً (بواوي، 2017)، وعليه نجد أن الأموال الرقمية وسيلة مبادلة دون أن تكون وسيلة تسديد (القادري، 2018).

ت. **البطاقة الذكية:** حيث تتألف من المعلومات المتعلقة بالزبون الممتلك لها، وتستطيع التخزين بمساحة واسعة، فهي تحوي جميع البيانات والتفاصيل وبالتالي يكون لديها القدرة على معالجة المعلومات وليس تخزينها فقط، كما أن المعلومات والتطبيقات قابلة للتحديث بدون الحاجة إلى تبديل البطاقة ولها القدرة على الاتصال بأجهزة الحاسب الآلي المختلفة عن طريق القارئ (قرومي، مرجع سابق).

ث. **الشيك الإلكتروني:** هو بديل للشيك الورقي وهو إلزام تشريعي بدفع كمية محددة من العملة في وقت معين لحساب فرد أو مؤسسة محددة، ويتم صرف قيمته عن طريق وسيلة رقمية مثل الحاسوب أو جهاز الموبايل، ويكون هناك توقيع رقمي في نهايته (باشا، 2020).

ج. **التحويلات المالية الإلكترونية:** هي وسيلة إعطاء تفويض لمصرف ما لأداء عمليات التحويلات المتعلقة بالنقود إلكترونياً من رصيد مصرفي إلى رصيد مصرفي ثاني، أي أن طريقة التصريف تحدث بواسطة الوسائل الرقمية من خلال الموبايل والحاسب بدلاً من استعمال الأوراق، وللتحويل الإلكتروني صورتين: الأولى تتضمن في التحويل المصرفي الإلكتروني بواسطة بنك واحد والثانية تكمن في التحويل بواسطة بنكين (باشا، 2020).

ح. **المحافظ الإلكترونية:** تمثل تطبيق رقمي يعتمد تخطيط آلية ضم العملية المتعلقة بالأموال وتشتمل المحافظ كل معلومات الزبون الذي يمتلك البطاقة بأسلوب مشفر، ويكون هناك

تثبيت لها على جهاز الحاسب الخاص أو حفظها على أي من الأقراص الملونة أو أي وسيلة يمكن من خلالها حفظ هذه المعلومات واستعمالها للتسديد من خلال أنظمة تعتمد الوسائل الحديثة عن بعد في كل الأمور التي تحتاج التسديد (خبازي، 2017).

ومن الجدير بالذكر في هذا المجال إلى إن خدمات الدفع الإلكتروني تنقسم من حيث طريقة الاستخدام إلى عدة أنواع، والتي تتضح من خلال ما يلي:

أ. خدمات بطاقات الدفع الإلكتروني:

تعرف بطاقة الدفع بأنها "البطاقة التي يمكن استخدامها من قبل حاملها وتكون مقبولة لدى التاجر لإتمام إجراءات الشراء أو لدفع أي التزامات أخرى"، كما توجد عدة أنواع للبطاقات هي بطاقة الائتمان وبطاقات الخصم (بطاقة السحب النقدي، بطاقة الدفع الفوري، بطاقة المتجر) (معهد الدراسات المصرفية، 2023).

ب. خدمات بطاقات الدفع المسبق:

هي وسيلة تسديد وأخذ مالي، يقوم بها مصرف أو شركة اقتصادية تعطي للشخص الذي يملك هذه البطاقات الحق في التسوق بالأجل على كفالة مصدر البطاقات أو عن طريق آخرين بكفالة خاصة تعطيه الحق بامتلاك ميزات محددة له (إدارة البحوث والتنمية، 2019).

تنقسم أنواع بطاقات الدفع المسبق إلى أربع أنواع رئيسية هي:

- المفتوحة: والتي تستخدم في جميع طرق الدفع والتحويل والسحب والتسوق الرقمي.
- شبه المفتوحة: هذا النوع من البطاقات لا يختلف عن البطاقات المفتوحة باستثناء أنه لا يمكن إجراء عملية سحب نقدي من خلالها.
- المغلقة: ففي هذا النوع من البطاقات لا يسمح بإجراء التسوق الرقمي أو السحب النقدي، ولكن تستخدم من خلال شركة أو تاجر واحد.
- شبه المغلقة: لا يسمح بالسحب النقدي من خلالها، ولكن يسمح استخدامها داخل مجموعة محددة من المطاعم والمنشآت والشركات (معهد الدراسات المصرفية، مرجع سابق).

ت. خدمات الدفع عن طريق الهاتف النقال:

يوجد عدة أساليب للدفع عن طريق الهاتف النقال من أهمها:

- المحافظ الرقمية: يتم استخدامها في البيع والشراء وتستخدم في تحويل الأموال، وتكون على الأغلب مرتبطة بتطبيقات البنوك أو الشركات النقدية أو الرقمية.
- الدفع باستخدام تقنيات الاتصال قريب المدى: حيث تمكن العميل من استخدام المحافظ الرقمية المشار إليها.
- المدفوعات الروتينية عن طريق جهاز الاتصال النقال مثل التحويلات الخاصة، وتسديد قيمة المستحقات، والتحويلات الخارجية، والمصاريف العامة التي يتم دفعها من خلال تطبيق أو منصة دفع خاصة بالجهة المستقبلية للأموال (معهد الدراسات المصرفية، مرجع سابق)

3. مزايا خدمات الدفع.

وهنا يمكن القول أن أبرز تلك المزايا هي الآتي:

- سهولة التعامل والثقة.
- يحافظ على الأموال من السرقة والضياع عند عملها.
- يحقق إيرادات للدولة من خلال العمولة التي يتم استقطاعها عند الدفع أو التحصيل.
- يضع حداً لمظاهر الفساد والعمولات التي تستقطع أو تدفع لغرض إكمال المعاملات أو إنجازها أو السكوت عن المخالفات (سدخان، 2020).

وعليه يمكن القول إلى إن مزايا خدمات الدفع تتجلى في ثلاث مجالات رئيسة هي:

أ. بالنسبة لحاملها: تعطي طرق التسديد الرقمي للشخص المعني خدمات كثيرة مثل بساطة وعدم تعقيد الاستعمال، فضلاً عن الثقة وحصول صاحبها على التأمين غير المدفوع لأوقات معينة، بالإضافة إلى أن حاملها يستطيع أداء عملياته التجارية بشكل آني فقط عن طريق إعطاء الرقم الخاص للبطاقة.

ب. بالنسبة للتاجر: تعد كفالة للحقوق الشخصية للتاجر، فهي تشارك في توسيع العمليات التجارية كما أنها استطاعت أن تخلصه من مشكلة متابعة ديون الزبائن، وذلك لأن هذا العبء يقع على عاتق المؤسسات المعنية.

ت. بالنسبة لمصدرها: تعتبر المزايا والضرائب من الأدوات الربحية التي تستفيد منها البنوك والمؤسسات المرتبطة بخدمات المدفوعات

4. مخاطر خدمات الدفع:

تزداد أهمية خدمات الدفع الإلكتروني مع توسع التجارة الإلكترونية وانتشار التكنولوجيا الحديثة، مما يسهم في تسهيل المعاملات المالية وتسريعها. ومع ذلك، ترافق هذه الخدمات مجموعة من المخاطر التي قد تؤثر على الأمان المالي للمستخدمين والشركات.

إن الخطر الذي يمكن أن تفرزه أنظمة الدفع الإلكتروني قد يفوق كل تصور ولعل تعدد مظاهر هذه المخاطر دليل على انسيابها وتشعبها بشكل يصعب السيطرة عليه، وهذا يدل على أنه لا توجد نقطة تنتهي فيها الفعل غير الشرعي الإلكتروني، فقد يتم من خلال الإنترنت سرقة المستندات والمعلومات وتزويرها، وتدمير مواقع المعلومات ونشر الإشاعات، وتشويه سمعة قطاع خدمات المدفوعات، مما يؤثر على مستوى الأمان والثقة لدى المستخدمين والمتعاملين مع قطاع خدمات المدفوعات (أحسن، 2009).

حيث أن أنظمة الدفع الإلكتروني التي يعتمد عليها قطاع خدمات المدفوعات ليست وسائل آمنة فهي تحتوي العديد من الأخطار التي تؤثر على مستوى الأمان والثقة لدى المستخدمين (كنزة وعائشة، 2022).

مخاطر أنظمة الدفع الإلكتروني التي تؤدي لحدوث الجرائم الإلكترونية:

أ. **مخاطر خرق أنظمة الأمان والحماية:** ويتمثل في الاختراق الممنوع إلى النظام الخاص بأرصدة المصرف بغية الاطلاع على البيانات الشخصية للعملاء واستعمالها بطريقة غير قانونية أو سرقة أرقام البطاقات الائتمانية بما يستوجب توافر استراتيجيات فعالة للكشف عن طريق القرصنة، حيث يقع على عاتق البنك مسؤولية كبيرة لتأمين المعلومات الموجودة على الوسائل الرقمية، واستخدام أفضل وأحسن البرمجيات واستخدام التشفير بدرجة عالية ومعقدة، ويقع أيضاً جزء من المسؤولية على العملاء في تأمين أجهزتهم واستخدام مضادات الفيروسات وعمل التحديثات بشكل فوري (سمير وراضية، 2022).

ب. **مخاطر التشغيل:** ينتج هذا النوع بسبب غياب وسائل التأمين الفعالة للنظم أو قلة كفاءتها أو بسبب عدم صحة بيانات أو عدم المنهجية في إدارة الأنظمة، وتتضمن:

- التأمين غير الوافي للنظم: وهي تتمثل بغياب طرق الأمان الفعالة لأنظمة أرصدة قطاع خدمات المدفوعات، الأمر الذي يسهل الاعتداء عليها بواسطة المخربين غير المسموح لهم بذلك، حيث يتاح

لهم الاطلاع على البيانات الشخصية للزبائن واستعمالها بطريقة مسيئة سواء كان ذلك من الوسط الخارجي لقطاع خدمات المدفوعات أو من الموظفين فيه.

- عدم ملاءمة بناء البرامج أو الإصلاح: وهي تنتج عن انعدام فعالية الأنظمة أو فشلها كربط العمل مثلاً للتعامل مع المستلزمات المتعلقة بالمستخدمين، والإبطاء في علاج المعوقات والإصلاح الدوري للأنظمة والبرامج وبشكل خاص إذا ما تم الاستعانة بأشخاص لا يعملون بالمصرف لإعطاء المساعدة الفنية، مما يؤدي إلى تسرب معلومات عن حسابات العملاء أو ظهور مشاكل فنية لمستخدمي شبكة الإنترنت، وبالتالي فقدان البنك لمصداقيته (شاهين، 2010).

- إمكانية اختراق الحسابات عن طريق اختراق بطاقات الدفع والتلاعب بالمعلومات.

- إساءة الاستخدام من قبل العملاء: حيث تتضمن عدم قدرة العملاء على استخدام الأنظمة وإساءة استخدامها وسماعهم لعملاء آخرين باستخدام حسابهم واستغلال هذا الحساب في أعمال مشبوهة (فريد وقاجة، 2018)، وينتج ذلك بسبب عدم معرفة المستخدمين والعملاء باستراتيجيات الأمان التي تمنع وقوع الاختراق أو تمكين المجرمين باختراق مواقع شخصية للزبائن مختلفين أو ارتكاب جرائم تبييض النقود باستعمال البيانات الخاصة أو قيامهم بإهمال استراتيجيات التأمين اللازمة.

- سلامة الآلية التجارية والبيانات الرقمية المصرفية: وهي أبرز مكونات أمن النظام ويجب على إدارات البنوك أن تعمل على تحسين قابلية الأنظمة للعمل والارتباط مع أنظمة أخرى داخل المنظمة نفسها، ومع المؤسسات الأخرى، ولكون الخدمة المصرفية متوفرة على مدار الساعة، فقد زاد ذلك من الضغوط التنافسية لكسب ثقة العملاء، وخفض من استعداداتهم لتحمل وقوع أخطاء (أسماء وحسنى، 2019، ص35).

- حيث يعد مفهوم الدفاع والأمان أحد الأقسام للتقنية الرقمية التي تعتمد عليها المعلومات التكنولوجية المصرفية بصورة رئيسية لتقديم خطط الحماية الملموسة والمعنوية لتأمين الحفاظ على الأنظمة والبرامج والبيانات، وعليه فإن حماية البيانات المحفوظة لدى المصارف هي الغاية الأسمى وهي المكون الرئيسي لثقة الزبائن فيه، حيث أن عمليات الدفاع والحفاظ على الأنظمة تكون ناقصة وغير ذات كفاءة مالم تقترن بالوصاية القانونية وذلك باعتماد نصوص قانونية تحافظ عليها من الاستغلال السيء للكمبيوتر والشبكات في اقتراف الأفعال غير الشرعية المتمثلة بالجرائم والإنترنت

والجرائم النقدية التكنولوجية لذلك من الضروري إيجاد خطة متكاملة لأمن معلومات البنك وعملائه والنظم المرتبطة به (سمير وراضية، 2022).

- مخاطر السمعة: ينتج هذا النوع في إمكانية وجود اتجاه غير إيجابي تجاه قطاع خدمات المدفوعات، مثلاً اختراق مواقع البنك على الشبكة مما يسيء إلى سمعة البنك مما يستوجب استراتيجية للاتصال لحماية سمعة قطاع خدمات المدفوعات (أسماء وحسنى، 2019). حيث أن الرأي السلبي للوسيلة بحد ذاتها سبب غياب القدرة على توفير خدمات الدفع الرقمية باعتماد مقاييس الأمان وعدم العلنية والموضوعية مع التتابعية والتعامل العاجل مع احتياجات العملاء، وهو موضوع من غير الممكن تجاهله إلا بواسطة الرقابة المستمرة من قبل المؤسسات والبنوك بتحديث التدقيق والاستمرار باختبار مقاييس أداء وسائل الدفع الإلكتروني (مشري وقاجة، 2018). كما يؤدي العجز في عمل المعاملات الرقمية الخالية من الخطأ إلى التأثير على سمعة المصرف والتي تبدأ بالانحطاط منذ اللحظة التي يعجز فيها عن إدارة أنظمتها المستخدمة، مما يولد غد العمل القناعة الكافية أن هذا البنك لا يستطيع أن يوفر الحد الأدنى من الأمان المطلوب، فإذا ما واجهت أمن المصارف مشاكل في خدماتها الإلكترونية فقد يؤدي ذلك إلى فقدان الثقة بها ليتوافر على أثره اتجاه غير إيجابي من ناحية المصرف، مما يؤدي إلى تعميم ذلك الرأي على بقية البنوك بسبب عجز المصرف عن العمل بفعالية في إدارة العمل داخله، أو حدوث اختراق مؤثر لها، وقد بدأت المصارف والبنوك تطرح مخاطر ناجمة عن اتساع الهوية في علاقتها مع العملاء مما جعلها تتعرض لعمليات نصب مختلفة، ذلك أن الخدمة المصرفية عبر الإنترنت تصعب مراقبتها بصورة دقيقة وهو ما يؤثر على حجم السيولة النقدية سواء بالزيادة أو النقصان، وحتى يمكن التحكم والحد من هذه المخاطر لابد من اتباع إجراءات التقنين، وذلك بالترخيص القانوني لأنظمة التسديد الرقمي والمعاملات التكنولوجية، كما لابد من التنسيق الدولي لتنظيم هذه المعاملات (سمير وراضية، 2022).

ت. **مخاطر التعرض:** وهي الأخطار الناشئة عن قصور جزء من البرمجيات في توفير التدقيق على كل ما يمكن أن تشمله الآليات المصرفية التكنولوجية، وكفالة عدم القيام بتغييرات على رسائل الزبائن خلال عبورها من خلال النوافذ الرقمية، وكفالة عدم تسرب المعلومات إلى العلن (شاهين، 2010).

ث. المخاطر الأمنية والقانونية للعملة الرقمية:

- المخاطر الأمنية: يعد البعد الأمني أبرز الأمور التي تقلق المتعاملين بأنظمة الدفع الإلكتروني، والجدير بالذكر أن هذه المخاطر لا تتعلق بالعميل فحسب، وإنما تمتد إلى التاجر ومصدر البطاقة الإلكترونية المملوكة للمستخدم والتي تتعرض للنهب أو التزوير، وقد يتم تزويرها من خلال تغيير البيانات المحفوظة على البطاقة أو على البرمجيات أو على القرص الصلب (الطيفلي، 2023، ص39). وقد يحدث الاعتداء الأمني للنقود الإلكترونية إما كنتيجة لعمل إجرامي عمدي مثل تقنية تفجير الموقع المستهدف ومحاكاة الموقع فضلاً عن تبديل المحتوى ومخاطر تزوير البطاقات واستخدام البنوك الرقمية في غسل الأموال (قيرة، 2022)، حيث أنه من شأن كل هذه التصرفات والتهديدات السابقة أن تؤدي إلى فقدان الأمان والثقة لدى المستخدمين.
- المخاطر القانونية: ينشأ هذا النوع أساساً من خلال انتهاك القواعد والتشريعات كالجرائم التي تلي تبييض العملة وإفشاء الأسرار السرية للعملاء، وانتهاك الخصوصية، ومن ناحية أخرى فإن المخاطر القانونية قد تتولد أيضاً عندما تقنن مستحقات وواجبات الفئات المتنوعة بالعملة الرقمية بطريقة ليست دقيقة، كذلك فإن موضوع وقاية المستخدمين يعد من أهم الأخطار القانونية التي يمكن أن تفرزها الأموال الإلكترونية (كنزة وعائشة، 2022).

ج. المخاطر المالية والتلقائية:

- ١- المخاطر المالية: تأخذ هذه المخاطر في حالة استعمال خدمات التسديد الرقمية عدة أشكال منها:
 - المخاطر الائتمانية: تحدث في عمليات التسوية الإلكترونية عندما يفقد القائم بالدفع جزء أو كل مدفوعاته بسبب إخفاق في توصيل التزاماته إلى الطرف الآخر، حيث تعد مخاطر الائتمان الأكثر شيوعاً في نظم الدفع الإلكترونية وذلك لتوفر مجموعة هائلة من الشركات للمستخدمين النظام بطريقة ليست واضحة وصريحة والمستخدم غير المباشر لا يكون عضواً في نظام المدفوعات ولكن يستخدم قطاع آخر عضواً في النظام، والسبب في تعرض المستخدم غير المباشر لهذه الفئة من الخطر هو فترة الإبطاء بين وقت تلقي قطاع خدمات المدفوعات ووقت إعلان بنك المستلم النهائي لها.
 - مخاطر السيولة: وهي من نظم التسويات الإلكترونية وتتمثل في عدم إمكانية تنفيذ أوامر الدفع على الرغم من أن بنك العميل يكون في حالة مالية قوية ولكنه غير قادر على دفع التزاماته لأسباب خارجة

عن إرادته، حيث أن مخاطر السيولة هي صيغة نموذجية لمخاطر التوقيت وترتيبات المدفوعات مما يؤدي إلى التأثير على الربحية.

-المخاطر التلقائية: إن عدم نجاح العاملين في برنامج تحويل العملة الرقمية أو ضمن السوق المتعلقة بالأوراق المتعلقة بالنقود في أداء واجباتهم، يؤدي عادة إلى عدم استطاعة الآخرين على القيام بالوفاء في الموعد المحدد (رميسة وشريفة، 2018).

ح. مخاطر البطاقات البنكية:

إن ظهور أنظمة الدفع الالكترونية عامل مساهم في ظهور الاختراقات غير القانونية والتي تتضمن كما يلي:

- انتحال شخصية الفرد: والتي تتم عندما يستغل البعض بيانات كالعنوان أو تاريخ الولادة أو التأمين الاجتماعي لشخص ما على مواقع الإنترنت بشكل سيء بغية توفير بطاقات مصرفية ضمانية، إذ أن تلك البيانات تسمح لهم بتوفير البطاقات المصرفية بواسطة التقنيات الرقمية غالباً عن طريق المؤسسات التي ليس لديها استراتيجيات أمنية قوية من خلال الإنترنت.
- جرائم السطو على أرقام البطاقات: حيث أصبح هذا الموضوع أمراً يسيراً لذلك كثرت هذه الجرائم التي جاء بعدها حالات تهديد مقترنة بطلب المال لإرجاع تلك الأرقام أو عدم استعمالها. (الطيفلي، 2023).
- عدم الدقة وإجراء بعض الأخطاء المعمولة بواسطة الموظفين في التعامل مع الفواتير ومع تكرار الأخطاء تفقد الثقة بين البنك والعميل.
- خطر السيولة على البنك في حالة الإفراط في استعمال البطاقة من طرف المتعاملين، حيث أن التماهي في استعمال البطاقة مع قلة الإيداعات لدى البنك، ووجود صعوبة في رفع سعر الخصم من طرف البنك المركزي يصبح الفرق موجوداً في العملية وغير مؤثر ويؤدي ذلك إلى وقوع البنك في مشكلة السيولة خاصة في حالة عدم دفع المستحقات في وقتها.
- المنافسة التي تتعرض لها المصارف من الشركات المصدرة للبطاقات الخاصة مما يقلل حجم المتعاملين مع المصرف أو البنك (كنزة وعائشة، 2022).
- غسيل الأموال: حيث تعد الشركات المصرفية الطريق المحبب للقيام بجرائم تبييض النقود بسبب فعاليتها وكلفتها القليلة في أداء التحويلات النقدية، ولما تتميز به التحويلات الرقمية من تعقيد وتشابك،

ولعل أكثر ما سهل من اقتراف هذه الجريمة هو ارتكابها بواسطة وسائل الدفع الحديثة (محمودي، 2021).

- استعمال الكمبيوتر في التلاعب بالمعلومات وذلك بإدخال بيانات زائفة من جانب المتحايل باختلاف الدائنين، كأجور يجب دفعها أو فواتير يجب سدادها، وذلك عن طريق اختلاف مدينين غير حقيقيين يجب عليهم سداد فواتير صادرة عن الحاسوب، أما المدين المعتدى عليه فلن يتمكن من إثبات كونه غير مدين لوجود فواتير معلوماتية، وهكذا يستغل المتحايل طرق الدفع الآلية للحصول على أموال غير شرعية. (الطفيلي، 2023).
- زيادة الإقراض والاقتراض بما يفوق الاستطاعة المالية وتخلف حامل البطاقة عن دفع مستحقاته في التاريخ المتفق عليه مما يؤدي إلى تحديد اسمه في اللائحة السوداء.
- إن حصول القليل من المخالفات من طرف حامل البطاقة البنكية أو عدم الوفاء بمستحقاته يؤدي إلى إلغاء تعامل المصرف معه، ويكتب اسمه في اللائحة المحظورة مما يؤدي إلى تحمل حامل البطاقة مشاكل كثيرة في عمله التجاري.
- أهم خطر يواجه مصدري البطاقات البنكية هو استطاعة حاملي البطاقات دفع الأموال المقترضة الملزمة لهم، بالإضافة إلى مسؤولية المصرف عن دفع ما يترتب عن فقدانها. (كنه، 2022).
- خ. **المخاطر الاستراتيجية:** تتعلق بالقوانين والاستراتيجيات والتوجيهات التي تتبعها الإدارات المسؤولة للمصارف والبنوك والمؤسسات المصدرة للبطاقات حيث تختلف عن بقية المخاطر كونها أكثر عموماً واتساعاً من المخاطر الأخرى، وتتسبب هذه الأخطار عن الاستراتيجيات الإلكترونية بسبب الخطط غير الصحيحة أو القصور الذي قد يحصل نتيجة تبني سياسات وخطوات تقديم هذه العمليات وتصميمها التي قد تقوم فيها الإدارات الأعلى، فمثلاً قد تنشأ مخاطر استراتيجية في حالة تباطؤ الإدارة في إدخال وسائل الحماية عند استعمال البرمجيات المعاصرة أو الإسراع في ذلك دون دراسة جيدة (مشري وقاجة، 2018).
- د. **مخاطر فجائية:** يؤدي هذا النوع من الأخطار إلى إشكالية في توفر الأموال وفي استراتيجية الديون المصرفية، وبالتالي عدم نجاح المساهمين في برنامج تحويل النقود الرقمية في الوفاء بالتزاماتهم سواء تعلق الأمر بالدفع أو السداد قد يؤدي إلى إضعاف قدرة المساهمين المختلفين لأداء مهامهم في الوفاء

بمستحققاتهم في الوقت المحدد مما يؤدي إلى عدم ثبات واستقرار العلاقات وهدم الاستقرار والأمان والثقة في الوسط المالي.

د. **مخاطر الكترونية:** وهي تتعلق بالتحويلات الرقمية المتسارعة خاصة فيما يتعلق بضعف إمام موظفي البنوك باستخدام الأنسب للتقنيات العصرية المرتبطة بالآليات البنكية على النحو الذي يؤدي إلى القصور في القيام بالاستراتيجيات الرقمية بطريقة مهنية (أسماء وحسنى، 2019). بالإضافة إلى مدى توفر الإدارة والموظفين من أصحاب الخبرة ذات الكفاءة المتعلقة بالمجالات البنكية الرقمية، ووجود مقاييس ثابتة ترتبط باحتمال تفادي عمليات الغش والخداع المالي وإثبات هوية وشخصية الزبون (شاهين، 2010).

ر. **مخاطر أخرى:** بالإضافة إلى المخاطر المذكورة سابقاً قد تتعرض أنظمة الدفع الإلكتروني إلى مخاطر أخرى تتمثل بما يلي:

- احتمال تعرض الأموال لأفعال جرمية كالسرقة والاحتيال وغيرها من الوسائل الإلكترونية وخاصة اختراق الحسابات.
 - العجز عن حماية الخصوصية المتعلقة بالعملاء بسبب عمليات الاختراق.
 - صعوبة تشغيل واستخدام بعض أنظمة المصارف الرقمية.
 - التقدم الرقمي المستمر مما يستوجب تحديث وتطوير الأجهزة والأنظمة بصورة مستمرة.
 - إمكانية تهريب الأموال إلى الخارج مما يهدد اقتصاديات العالم.
 - عدم الاتفاق على سعر معين فيما يخص العملات الإلكترونية، وما إذا كان ممكناً وجود سعر صرف موحد للعملات الإلكترونية التي تصدر في البلدان المختلفة وأيضاً إذا ظهرت وحدات نقد رقمية مقبولة التداول عالمياً فقد تفقد العملات الوطنية معناها وسيادتها على أراضيها.
 - عجز التشريعات عن استيعاب والإحاطة بالآليات الإلكترونية نتيجة سرعة التغير والتقدم المستمر.
 - عدم قدرة المصرف على فرض رقابته على تحركات الأموال وخاصة أنها تعرف بالسرعة.
- نستنتج مما سبق بأن الحياة تتطور وتتطور معها الأنظمة والوسائل الكفيلة بتحريك عجلتها بشكل يومي للحاق بهذا التطور، ولا توجد مؤسسة أو مصرف أو بنك أو قطاع مدفوعات أو خدمات بعيداً عن هذا التقدم الذي يشمل كافة مناحي الحياة، والذي أضفى الطابع الرقمي التكنولوجي على جميع معاملاته وأنظمته، هذا التطور التكنولوجي الهائل والسريع، حيث اتجهت جميع البنوك وقطاع خدمات المدفوعات

بجميع مؤسساتها نحو العالم الرقمي بأنظمتها ووسائله وتقنياته الرقمية، والذي أتاح سرعة التعاملات الإلكترونية وتوفير التعب والزمن ، وتبسيط الإجراءات، والتحول نحو البطاقات المصرفية والنقود الرقمية وغير ذلك، ولكن هذه الأنظمة لابد أن تصيها بعض المخاطر التي تحول دون تحقيق الكفاءة في العمل، فعلى الرغم من الميزات الكثيرة التي تتصف بها إلا أنها تعاني من بعض المخاطر المتعلقة بأنظمة حماية أمن البيانات، والحفاظ على سرية العملاء وغير ذلك، تلك المخاطر تجعل من الضروري والواجب على أي قطاع من قطاعات خدمات المدفوعات أن يضع على عاتقه مسؤولية حماية العملاء، وتقديم التحديثات المستمرة لأنظمة الدفع الإلكتروني المعتمدة لديه، حتى يحافظ على ثقة وأمان العملاء الذين يتعاملون معه، والحفاظ على جودة خدماته المقدمة بالشكل الذي يعطي انطباعاً جيداً لدى العملاء ويساعدهم على تكوين رأي إيجابي في الخدمات المقدمة من خلال أنظمة الدفع الإلكتروني، وبالتالي تعميم تجربتهم ، حتى يتمكن قطاع خدمات المدفوعات من بناء الثقة والاستقرار في عمله والنهوض بأهدافه ، وبالتالي تحقيق الأرباح، والتخلص من الجرائم الإلكترونية التي تجد ثغرة في أنظمة الدفع الإلكتروني لإحداث الخلل والاختراق، وبخاصة في نطاق السباق المستمر بين الشركات والتي تختبرها الأسواق المالية.

5. العوامل التي تسهم في تقليل مخاطر خدمات الدفع.

إن نظم الدفع الإلكتروني تطورت بتطور البيئة التشريعية والشراكة الذكية بين قطاعات العمال في المصارف والاتصالات والتجارة، وشكلت بطاقات الائتمان المصرفية وسيلة للبرامج البنكية من خلال البنك الآلي وتطورت حتى المعاملات الرقمية في نافذة المصرف الآلية، كما دفعت نقاط البيع إلى تطوير عمل بطاقات الائتمان كوسيلة للشراء المباشر، وساهمت أيضاً في عملية الشراء غير المباشر عن طريق الإنترنت في المعاملات الرقمية المحلية والدولية مما ساعد على تطور التجارة الإلكترونية (الأمين، 2014).

وعليه يمكن القول إلى إنه لتقليل مخاطر خدمات الدفع لابد من اتباع فئة من القواعد الرقابية التي تمارسها الجهات المختصة، والتي تتجلى من خلال الآتي (سدخان، مرجع سابق):

أ. **حماية البيانات والمعلومات:** أي أن تكون البيانات سليمة وسرية وتمنع الزبائن غير المصرح لهم بالدخول إلى هذه البيانات، وذلك لأنه من الضروري أن تتم تقدير خصوصية البيانات الشخصية للزبائن على اعتبارهم العملاء بالإضافة إلى تقدير حقهم في حماية سرية شخصيتهم ويتطلب ذلك

- الالتزام بعدم إذاعة أو إتاحة أي معلومات تصف حياتهم الخاصة وكذلك المعلومات البنكية، وذلك من خلال طلب المشتريات والبضائع، بالإضافة إلى المعلومات الخاصة بالعمل واتجاهاته، وهي التي يمكن مراقبتها بواسطة الشركات بطريقة الكترونية (محمودي، 2021).
- ب. **توفير الثقة والضمان للمستخدمين** لضمان قبول المستخدمين استخدام هذا النظام كبديل عن النماذج الروتينية في خطط التسديد والتحصيل من خلال الفوائد.
- ت. **إلزام الشركات والمصارف المرخصة بتوفير بنى تحتية موثوقة** وفعالة من حيث القيمة المادية والزمن، وكذلك الدقة في العمل مع سهولة الاستخدام وأن تكون محصنة وفي مأمن من الاختراق.
- ث. **إيجاد منظومة تشريعية متكاملة** لتنفيذ متطلبات أخذ المستحقات والدفع الإلكتروني بالصورة الصحيحة، وذلك بعد التقدم الحاصل في أنظمة الدفع الإلكتروني فلم تعد تعمل في داخل البلد فحسب وإنما أصبحت ذات صفة دولية يمكن استخدامها بيسر وسهولة.
- ج. **التشفير**: يؤلف جزءاً هاماً كطريقة من طرق تأمين المعاملات الرقمية بشكل عام بفضل ما يحققه من سرية البيانات إذ يعرف التشفير على أنه استراتيجية يتم من خلالها تحويل معلومات واضحة إلى معلومة غير واضحة ومبهمه من خلال خطوات وقواعد سرية بحيث يمكن ارجاعها إلى حالتها الأساسية (باشا، 2020).
- ح. **اتباع التذييل والتصديق الرقمي**: وذلك بهدف الحفاظ على المعلومات الخاصة وتأمينها في البيئة الرقمية وتجسيد التجارة الرقمية (محمودي، 2021).
- خ. **الشهادات الرقمية**: وهي عبارة عن وثائق الكترونية تثبت هوية العملاء عبر الانترنت ويتولى إصدار هذه الشهادات جهة موثوق فيها تسمى سلطة إصدار الشهادات، حيث تحتوي كل شهادة رقمية يتم إصدارها على قاعدة بيانات مهمة تتعلق بمالكها وبالسلطة التي أصدرت هذه الشهادة مثل اسم حامل الشهادة والمفتاح العام لحامل الشهادة واسم سلطة إصدار الشهادة الرقمية ورقم متسلسل وتاريخ الإصدار ومدة صلاحية الشهادة (خبازي، 2017).
- د. **الرقابة الإدارية لإيقاف المخاطر الرقمية** وذلك لحماية الدفع الإلكتروني وذلك باتخاذ إجراءات خاصة تتمثل أساساً في وضع قيود على القيم المخزنة على وسائل الدفع (باشا، 2020).

ثانياً - مدخل للجرائم الإلكترونية

١ - مفهوم الجرائم الإلكترونية:

هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلاً وذلك باستخدام شبكات الإنترنت من خلال غرف الدردشة والدخول غير المرخص إلى حساب الإنترنت ومختلف الوسائل الرقمية بهدف إلحاق الضرر بشخص أو فئة من الأشخاص وحتى لدولة من الدول تكون ضمن برنامج الاستهداف الحربي أو الاقتصادي أو الإضرار بسمعتها، حيث يبقى الهدف واحد وهو الكشف عن قضايا متستر عليها أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب، كما تعرف الجريمة عن طريق الوسائل الإلكترونية بأنها كل عمل ليس قانوني يكون فيه هناك معرفة كبيرة بالتكنولوجيا الرقمية اللازمة للقيام به من جهة متابعته، وتنفيذه من جهة أخرى حيث يجب أن تتوفر معلومات وخبرة هائلة بتكنولوجيا المعلومات لاقتراف الفعل غير الأخلاقي إلكترونياً لمتابعتها تجريم الفاعل (عائشة، 2017).

ويتضمن هذا المفهوم كافة أنماط العمل غير القانوني الذي يتم باستعمال الكمبيوتر، وهي عمل غير قانوني غرضه تصوير أو اختراق المعلومات المحفوظة ضمن الكمبيوتر أو تعديلها أو محوها أو التي تنتقل من خلاله، فهي عمل غير أخلاقي تكون الخبرة بالكمبيوتر وبرامجه جوهرية للقائم بهذه العملية، حيث تشير إلى الاختراقات غير الشرعية التي يمكن أن تنفذ باستخدام التقنيات الرقمية بهدف كسب الفائدة، كما عرفت من ناحية أخرى بأنها كل عمل يتضمن التعدي على النقود الملموسة أو المحسوسة ويكون واقعاً بصورة قسدية أو غير قسدية من خلال استخدام الوسائل الرقمية (العجمي، 2014).

وتشير الجريمة الإلكترونية إلى كل اختراق للمعطيات التكنولوجية في سريتها أو في وفرتها أو في سلامتها وتكاملها، وذلك بالاطلاع غير المشروع عليها أو حذفها أو إدخال معطيات أخرى عليها أو تعطيل أنظمة معالجتها، فالجرائم الإلكترونية تقع على المعطيات أو البيانات الموجودة ضمن أنظمة التعامل الرقمي مع المعطيات، وهي لا تقتصر على الأنظمة المتضمنة في الأجهزة الإلكترونية وإنما تشمل كل نظام يحتوي هذه المكونات الملموسة وغير الملموسة، فيدخل فيه مثلاً بطاقات الائتمان بما تحويه من معلومات لأن هذه البطاقات جزء من نظام صالح لكي يقرأ ويسجل المعلومات على شريحة عندما يوضع في اتصال مع هذا النظام (خليفة، د.ت).

ولهذا العمل غير القانوني أسماء مختلفة منها:

- جرائم الأجهزة الذكية
- جرائم التقنية الرقمية
- الجريمة السيبرانية
- جرائم أصحاب الياقات البيضاء (مرعي، 2016).

2- أركان الجريمة الإلكترونية:

لها ثلاثة أعمدة تتمثل بما يلي:

أ. الركن الشرعي: وهو السمة القانونية للفعل وتشتمل على قانون تضمنين جرمية الفعل وتحقيق العقوبة فيها بصيغة متوفرة في القانون المتمثل بالتشريعات للوقاية من الأعمال الإجرامية المتعلقة بالوسائل الرقمية الخاصة بالاتصالات ومعالجتها (عائشة، 2017).

ب. الركن المادي: يتطلب الركن المادي في الجرائم الإلكترونية توفر وسط رقمي ويعني ذلك فئة المواد من مواضيع وصور وغيرها محفوظة بطريقة رقمية ويمكن توفيرها من خلال مجموعة وسائل، حيث يتطلب الركن المادي معرفة هذا العمل والبداية فيه وعاقبته، فمثلاً يقوم مفتعل الجريمة بتوفير جهاز الكمبيوتر من أجل ضمان وقوع هذا الفعل فيقوم بتنشيط برنامج دخول غير مصرح به أو أن يعتمد إلى تصميم هذا البرنامج بنفسه، كما يحتاج إلى تجهيز مواقع تحمل ضمنها عناصر مشبوهة وفيروسات وتنشيتها على الجهاز المضيف كما يمكن أن يقوم بجريمة تصميم برامج ضارة تمهيداً لبثها، ولكن ليس كل فعل جرمي يستوجب خطط مسبقة، فالسلوك غير الأخلاقي قد يتحقق بمجرد ضغط زر في لوحة المفاتيح الملحقة بالحاسب فيتم تدمير نظام مواقع الزبائن في أحد البنوك (الربيعي، 2024). حيث يحوي المواد الملموسة في الفعل الإلكتروني الجرمي التي تظهر إلى الوسط الخارجي (عائشة، 2017).

ت. الركن المعنوي: هو الحالة الداخلية لمرتكب هذا العمل والصلة الواصلة بين المكونات الملموسة للجريمة الإلكترونية وشخصية مرتكب الفعل الجرمي، كما أن الأصل أنه لا فعل جرمي بدون عماد

محسوس ، فهذا الأمر هو وسيلة المشرع إلى تخصيص المسؤولية عن هذا الفعل حيث يتعين توفر الركن المعنوي في الجريمة الإلكترونية بالرغم من أنها لا ترتكب في عالم مادي وإنما في عالم افتراضي، فيجب أن يكون الجاني عالماً بأن الفعل الذي يأتيه أو سلوكه المادي يجرمه القانون وعلى الرغم من توافر هذا العلم لديه تتجه إرادته إلى إثبات أن هذا الفعل قاصداً لتحقيق نتيجته، وقوام الركن المعنوي هو الأساس الداخلي لمكونات الجريمة والتحكم النفسي فيها حيث أن الركن المعنوي في جوهره قوة نفسية، وهذه القوة هي الإرادة وهي جوهر الركن المعنوي وإثباته يتوقف على مدى صعوبة فهم شخصية مرتكب الجريمة، فإذا اتخذت هذه الإرادة شكل العمد في العمل وصفت بأنها جريمة قسدية (الربيعي، 2024). كما أن للجريمة الإلكترونية كغيرها من الجرائم أطراف تتمثل في الجاني وهو المجرم الإلكتروني، وبهذا المعنى يكون الجاني شخصاً طبيعياً ذا أهلية وقدرة على تحمل العقوبة أو جهة معنوية مؤسسات خدمات المدفوعات أو الشركات وغيرها من المؤسسات والشركات التي تعتمد على الحاسب الآلي، علماً أن لها محلاً يتمثل في المعلومات والأجهزة والأشخاص والجهات (عائشة، 2017).

3- خصائص الجريمة الإلكترونية

أ. خطورة الجريمة الإلكترونية: تتطوي على خطر جسيم وذلك لوقوعها على العميل في شخصه ، كما تمس الشركات في نشاطها الاقتصادي خاصة، ويقع ضررها على أمن البلاد الوطني مع ما في ذلك من خطر المساس بالبيانات والأسرار المختلفة، وفي جانب آخر فهي جرائم تنتهك حرمة الحياة الخاصة، فالاطلاع على خصوصيات الأفراد جريمة يعاقب عليها القانون كونها تنتهك حق الأفراد في حماية خصوصياتهم، ومن ناحية أخرى فإن الاختراقات المتكررة التي تتم لأنظمة الحواسيب في الهيئات الرسمية للعديد من الدول أثبتت أنه مهما بلغ تقدم الدول فإنها تبقى معرضة لتلك الاختراقات والجرائم الإلكترونية (مقلاتي و مشري، 2021).

ب. الجريمة الإلكترونية جريمة تتخطى المسافات: أدى توسع شبكة الإنترنت إلى احتمالية وصل أجهزة كمبيوتر متعددة بالشبكة العالمية الرقمية من دون أن ترتبط بقواعد التاريخ والموقع لذلك من السهل أن يكون مرتكب الجريمة في موقع معين والشخص الذي ارتكب بحقه هذا الفعل في موقع آخر

وبذلك ظهرت أهمية توفير تشريع قانوني عام يتناسب مع القانون ضمن كل بلد للقضاء على هذا النوع من الأعمال ومعاقبة القائمين عليها (العجمي، 2014).

ت. عدم سهولة اكتشاف الجريمة الإلكترونية وإثباتها: تتصف الجريمة الرقمية بأنها غير واضحة في العموم بحكم أن الشخص الواقع بحقه هذه الجريمة لا ينتبه لها رغم أنها قد تحدث أثناء توفره على الشبكة، وذلك لأن مرتكب الجريمة لديه مهارات تقنية تجعله ماهراً في ارتكاب الجريمة بشكل محترف كنشر برامج ضارة، والتجسس والتعدي على المعلومات، ويمكن إرجاع الأسباب التي تجعل تحديدها أمراً بالغ الصعوبة إلى عدم تركها لدلائل كما في الأحوال العادية فهي تتم في بيئة رقمية، كما تمكن المهارات الرقمية من إخفاء آثار الجريمة من خلال العبث غير الظاهر في البرامج الرقمية، وبالتالي محو آثاره مما يخلق صعوبات بالغة لسلطات البحث والتحري في ملاحقته (مقلاتي ومشري، 2021).

ث. الاعتداء في الجريمة الإلكترونية يشمل معطيات الحاسب الإلكتروني: حيث يقع الاعتداء على الحاسب وملحقاته كأجهزة الإدخال والإخراج، حيث تحدث الاختراقات الإلكترونية في الوسط الرقمي للبيانات حيث يتطلب أداؤها العمل مع معلومات مهيئة لاختراق البرنامج الإلكتروني بهدف تحليلها بطريقة رقمية مما يمكن المستخدم من القدرة على تسجيلها عن طريق الآليات المطلوبة والتي تتضمن احتمالية تعديلها أو محوها أو استرجاعها، حيث أن هذه العمليات مرتبط بشكل كبير بحدوث الفعل الإجرامي إلكترونياً (المطيري، 2023).

ج. الجرائم الإلكترونية تتم عبر الوسائل الرقمية الحديثة: حيث يتطلب ارتكابها وجود حاسب آلي ومعرفة تقنية، ويعد الكمبيوتر الأداة الأساسية لحدوث كافة الاختراقات الرقمية والمقصود من وجوده هنا أن يستعان به كوسيلة لتنفيذ هذه الجرائم، حيث يطال الاعتداء على ما يمكن أن يسمى فن الحاسب الآلي كتموير برامجه وسرقتها وتقليدها أو العبث ببيانات الحاسب أو المعلومات المخزنة (مقلاتي ومشري، 2021).

ح. الجرائم الإلكترونية ناعمة ومغرية للمجرمين: إذا كانت بعض الجرائم العادية تحتاج من مرتكبيها إلى قوة عضلية للقيام بها فإن هذه الأعمال لا تحتاج إلى تلك القوة العضلية، وإنما تحتاج إلى مهارة رقمية، والجاني في سبيل تنفيذها لا يحتاج من الوقت إلا قدراً بسيطاً أو دقائق معدودة ولا يحتاج من القدرة الجسمية سوى تحريك الأصابع على وسائل الإدخال ويتسبب ذلك في حدوث خسائر فادحة،

رغم أن هذه الجريمة قد لا ترى بالعين ونعومتها وما تحققه من فوائد ومن تحقيق لحب الفضول عند البعض، كل ذلك جعلها من الجرائم والجاذبة للمجرمين (خليفة، د.ت).

4- أنواع المجرمين في الجريمة الإلكترونية:

أ. المتطفلون: مثل الأشخاص البارعين في اختراق حسابات العملاء حيث يكونون من ذوي الخبرة في استخدام الحاسب الآلي ولديه حب الاطلاع على حسابات الآخرين الشخصية بوسائل ليست أخلاقية مما يعني أنهم جهات غير مرغوب بهم لدى الآخرين وأغلبهم ما يكون هدفهم اختراق مواقع الحسابات من أجل تحقيق الشخصية (العجمي، 2014). حيث أن هذا النوع من مجرمي هذه الأنواع متطفلون يتحدون استراتيجيات الوقاية للبرامج لكن ليس عندهم دوافع تخريرية وإنما هدفهم التحدي وإثبات مهارتهم (المطيري، 2023).

ب. المحترفون: وهم الأكثر خطراً بين مجرمي التكنولوجيا حيث تكون غايتهم في بعض الأحيان الاختراق لتحقيق الفائدة غير الأخلاقية المرتبطة بالفوائد المالية وذلك من خلال الاعتداء على رصيد المصارف وأحياناً أخرى تكون غايتهم الوصول إلى أهداف سياسية والتعبير عن موضوع معين (العجمي، 2014، ص22). حيث يتميز هذا القسم من مجرمي الجرائم الإلكترونية بالمهارة الهائلة والخبرة والتنظيم والتخطيط للأنشطة المرتكبة لذلك فإن هذا النوع يعد الأخطر بين الفئات الأخرى وتهدف اعتداءات القائمين بها في الأصل إلى توفير النفع لهم أو للجهات التي وجهتهم (المطيري، 2023).

ت. الحاقدون: وهؤلاء ليس لديهم أي أغراض للجريمة ولا يهدفون لتحقيق فوائد من أي نوع ولكن تكون غايتهم لدوافع شخصية معينة عائلية أو نفسية (العجمي، 2014). حيث أن هؤلاء لا يسعون إلى تحقيق هدف مالي، ولهذا فإنهم يصنفون إما إلى مستخدمين للنظام بالصورة التي تصف صلتهم بالمؤسسة التي تجري فيها أحداث هذه الأفعال، أو أن يكون الهدف هو القيام بمعركة من خلال الوسائل الرقمية والتي تنفذها جهة أخرى منافسة (المطيري، 2023).

5- أهداف الجرائم الإلكترونية:

- الحصول على البيانات بشكل غير قانوني بهدف سرقتها وتعديلها بما يمكن الجاني من الوصول لغاياته.

- إمكانية الحصول على البيانات الخاصة ببرامج المعلومات والقيام بإيقاف عملها.

- الحصول على البيانات الخاصة للمؤسسات التي تستخدم الوسائل الرقمية كالمصارف وتهديدهم من خلالها.
- الربح المالي أو النفسي غير الأخلاقي بالوسائل الرقمية المعلوماتية مثل آليات الاعتداء وتعطيل الحسابات. (مرعي، 2016).

6- أنواع الجرائم الإلكترونية المرتبطة بخدمات الدفع الإلكتروني

تظهر بصيغتين:

الأولى: أفعال تحصل من خلال استعمال جهاز الكمبيوتر مثل اعتماد الأجهزة التقنية في أساليب الغش والاحتيال المتعلقة بالنقود وتزوير الأوراق القانونية والاختلاس أو استخدام الأجهزة الإلكترونية لأهداف الوصول غير الشرعي لقاعدة البيانات المثبتة على نظام إلكتروني آخر، من خلال وسائل الانترنت غير المحلية أو بطريقة واضحة بهدف تحقيق مكاسب مالية أو غيرها أو السيطرة على المعلومات.

الثانية: جرائم حاصلة على جهاز الكمبيوتر بمكوناته المرتبطة بالجانب المعنوي كجرائم تعديل أو تقليد أنظمة جهاز الكمبيوتر وجرائم تعطيل المعلومات المرتبطة بجهاز الكمبيوتر نفسه، بالإضافة إلى الأفعال المعروفة كالسرقة والإتلاف (العجمي، 2014).

ومن أنواع الجرائم الإلكترونية المرتبطة بخدمات الدفع ما يلي:

أ. جرائم التجارة الإلكترونية: أدى الاستخدام الواسع لشبكة الاتصال والاستفادة من تطبيقات العصر الرقمي إلى رواج عمليات البيع والشراء عبر الإنترنت، التي وفرت الكثير من الميزات وفي الوقت نفسه ازداد معها حجم الجرائم المرتكبة في سياق معاملات تلك التجارة في ظل تخلف الآليات التقليدية وعجزها عن التعامل معها، وخاصة أن عمليات البيع والشراء عبر الإنترنت تعتمد الطابع الافتراضي، حيث يتم تسليم الخدمات والمنتجات إلكترونياً، كما أن عدم وجود مستندات ورقية بخط اليد يحدث مشكلة عدم التمييز بين الرسالة الأصلية وصورتها، مما يضخم حجم جرائم التزوير، كما تحدث العديد من وسائل السطو وقرصنة البيانات الخاصة عبر الإنترنت والتي يكون ضحيتها العميل (مقلاتي ومشري، 2021).

ب. **جرائم السطو على أرقام بطاقات الائتمان:** تتمثل في اعتماد التذاكر الائتمانية رقمياً حيث يقوم المتسللون باختراقها باعتبارها نقوداً إلكترونية خاصة أن السيطرة على البطاقات الخاصة بالائتمان أمر سهل، حيث أن مجرمي تذاكر الائتمان يستطيعون الحصول على مئات الألوف من أرقام البطاقات في مدة قصيرة من خلال وسائل الاتصال ومن ثم التصرف بها بطريقة غير أخلاقية (راشد، 2018).

ت. **انتحال شخصية الفرد:** وتتم عندما يستغل اللصوص البيانات الشخصية للمتعاملين مع البنك أو أي قطاع خدمات المدفوعات وذلك من أجل الحصول على تذاكر مصرفية اعتمادية، حيث أن تلك المعلومات توفر لهم التقدم بعروض لعمل التذاكر الاعتمادية المصرفية من خلال العالم الرقمي غالباً ومن خلال المؤسسات التي ليس لديها قوانين قاسية تحكم المعاملات الإلكترونية (وهيبة، 2010).

ث. **الأفعال الحاصلة على النقود ووسائل الاتصال:** ويقصد بها الأفعال التي تتضمن السطو على النقود والمعلومات والبرامج مثل الحصول على النقود من خلال آلات الصرف الإلكتروني، حيث أنه من الممكن أن يعتمد شخص ما بتصميم بطاقة مزورة والسحب عليها من خلال أحد المصارف، كما تشمل الأعمال الإجرامية إلكترونياً وسائل الاتصال وخطوط شبكات الاتصال فالشخص الذي يقوم بارتكاب هذه الأفعال يعتمد إلى تزيف بطاقات الهاتف أو قد يعتمد إلى توفير صورة طبق الأصل من بطاقات التحويل التي لم تستخدم عن طريق حسابات ومواقع الشركات والمؤسسات. (العفيفي، 2013).

ج. **تزوير البطاقة البنكية:** يعد التزيف في نطاق التعامل الإلكتروني مع المعلومات من أخطر الجرائم المرتبطة بخدمات الدفع الإلكتروني، وذلك تبعاً للطابع التقني والفني الذي تتميز به من جهة وإلى صعوبة اكتشاف المزور وإثباته من جهة أخرى، حيث تعد البطاقة المصرفية طريقة من طرق الدفع الإلكتروني، حيث أن الغاية الأساسية من تزوير البطاقة البنكية هو الانتفاع بالخدمات التي تؤديها كوسيلة من وسائل الدفع الإلكتروني للقيام بالاستيلاء على أموال الغير، حيث يتم اصطناع بطاقة كاملة بعد الحصول على معلومات تتعلق بأسماء وأرقام أصحاب البطاقات الصحيحة والمتداولة بواسطة أشخاص مجندين لذلك من خلال الحصول على الشيفرة الأساسية المتعلقة بالتذكرة الأصلية (راشد، 2018).

ح. جرائم الاعتداء على الأشخاص: حيث تتعلق بالأفراد من خلال إمكانية التجسس على حياتهم الشخصية واختراق حساباتهم وتهديدهم وابتزازهم بهدف تشويه السمعة والإساءة للأشخاص (العفيفي، 2013).

خ. جريمة السرقة والسطو على أموال البنوك: حيث أنها سرقة مال منقول تعود ملكيته للغير بدون موافقته بهدف الحصول عليه، وتتم سرقة العملة الرقمية عن طريق السيطرة على البيانات الخاصة والاستخدام السيء لها مثل الاسم والعنوان والأرقام الخاصة بالمستهدفين والاستعمال غير القانوني لشخصية الشخص المستهدف ليبدأ بها عملية الاختلاس غير الظاهرة عبر الوسائل الرقمية بحيث تؤدي أخيراً إلى تقديم العملة الإلكترونية إلى المجرم بواسطة التحويلات المصرفية (راشد، 2018).

د. غسيل النقود: يعد غسيل النقود إحدى طرق الأعمال الجرمية المالية وهو موضوع يتعلق بالعملية الجرمية العالمية المنسقة، وبخاصة متاجرة المواد الممنوعة والإرهاب العالمي وتهريب الأجهزة والتزييف، وتعد عملية تبييض العملة الرقمية من الأفعال الدولية التي تنال اهتمام جميع الدول، وتراهن على مواجهتها جميع الهيئات على اختلاف أنواعها، ولأن الجهاز البنكي هو الأداة الفعالة لإعطاء الخاصية الشرعية على الأموال المشبوهة، فإنه صار من المعتاد أن توجه أعمال القائمين على تبييض النقود إلى المصارف على أمل إجراء سلسلة من العمليات المصرفية المعقدة التي تتضمن إدخال وسطاء وشركات وهمية والبحث عن ملاذات آمنة يصعب فيها مراقبة الودائع المالية لتندمج ضمن التحويلات النقدية وأنشطة البورصات والمبادلات المتعلقة بالنقود ولا يمكن لذلك أن يتم بسرعة واحترافية إلا إذا جرت الاستعانة بما تكفله البرامج التكنولوجية والتي تزيد من نسبة نجاح تلك العمليات، والواقع يشير إلى أن الأضرار الناجمة عن هذه الأعمال لا تقتصر على الأمور المحسوسة فقط بل تمتد إلى الجوانب الإنسانية والأمنية باعتبارها جريمة مركبة تأتي لاحقة لجريمة أخرى (مقلاتي ومشري، 2021).

ذ. السطو على وسائل السحب الإلكتروني للأموال:

تحدث في حالة استعمال الجهاز لسحب ما يفوق المبلغ الأصلي إذا تم بواسطة مالك التذكرة، فالموضوع في هذه الحالة لا يفوق كون الموضوع مالي بين الشركة والزبون لأن توفير المبلغ بطريقة غير قانونية

تم دون موافقة الجهة المالية طالما أنها تعلم بأن الجهاز غير متعلق بالحد الأعلى لرصيد الزبون حتى لا يفوقه (خيازي، 2017).

ر. التحويل الإلكتروني غير المشروع للأموال: حيث تحصل عملية التحويل الإلكتروني غير القانوني للأموال من خلال توفير الشيفرة المدونة في برامج الحاسبات الآلية المرتبطة بالمستهدف مما يسمح للجاني بالتوغل في البرنامج الأمني، وعادة ما يكون هؤلاء من الموظفين المختصين بإدخال المعلومات في وحدة تخزين الجهاز أو من خلال المتصلين على الإنترنت خلال عملية مشاركة المعلومات (راشد، 2018).

ز. الاستعمال غير القانوني للبطاقة منتهية الصلاحية: الأصل أن البطاقة المستخدمة في الدفع الإلكتروني تكون صالحة لمدة معينة ويتم تجديدها، لذلك يجب على حامل البطاقة أن يجددها بعد انتهاء المدة وتسليم البطاقة القديمة واستلام البطاقة الجديدة، فإذا قام صاحب البطاقة بالاحتفاظ بها واستخدامها بشكل غير مشروع فإنه يعتبر مقترفاً لجريمة إلكترونية.

س. الاستخدام غير القانوني للبطاقة الضائعة: ويتحقق ذلك من خلال استخدام اسم العميل صاحب البطاقة المفقودة أو المسروقة في الجهاز، فقد ادعى لنفسه وصفاً كاذباً أي أنه يحق له أن يسحب الرصيد باعتباره صاحب الحساب (سدخان، 2020).

التطور التقني الذي تشهده البيئة الرقمية، جعل العالم شبكة مفتوحة تسهل تدفق المعلومات من خلالها، وقد سعت جميع قطاع خدمات المدفوعات إلى استخدام أنظمة الدفع الإلكتروني في التعاملات البنكية مع العملاء، فكان لهذه الأنظمة إلى جانب ميزات عيوب وثغرات ساهمت في انتشار الجرائم الإلكترونية بأشكالها المختلفة التي يقترفها مجرمون محترفون على دراية تامة بالتقنيات الرقمية، ولأهداف كثيرة منها تحقيق الربح المادي أو إثبات القدرة على اختراق الحسابات، كل تلك الممارسات والجرائم الرقمية التي تستهدف أنظمة الدفع بوسائل رقمية تستوجب وضع سياسات واستراتيجيات صارمة وفعالة لتحقيق الأمان المعلوماتي للعملاء، والحفاظ على حياتهم وبياناتهم الشخصية من الاعتداء.

ثالثاً- العلاقة بين مخاطر أنظمة الدفع الإلكتروني وحدوث الجرائم الإلكترونية

شهد الاقتصاد الدولي المعاصر الذي بات يعرف بالاقتصاد المعلوماتي الرقمي تطورات تكنولوجية مستمرة انعكست بآثارها الإيجابية والسلبية على أداء القطاع البنكي حيث تمكن هذا الأخير من إيصال خدماته المصرفية إلى زبائنه ببسر وسرعة فائقة، ومن ناحية أخرى سهل ذلك التطور على العصابات الإجرامية (القرصنة) إمكانية الدخول إلى البرنامج الرقمي والمالي وإلحاق الضرر الكبير سواء على المستوى الفردي كحامل البطاقة الائتمانية أو على مستوى البنك من إلحاق خسائر فادحة عليه، وانطلاقاً من الدور الإيجابي الذي تلعبه أنظمة الدفع الإلكتروني فإنها قد تتعرض للتلاعب والتحايل من الاستخدام غير المشروع مما يمثل تهديداً مباشراً للعلاقة مع العملاء ويعزز الأمن والثقة تجاه التعامل مع البنك، مما يؤدي إلى فقدان الثقة والأمان وبالتالي تشويه سمعة البنك (صقر، 2020).

كما أن انتشار الجرائم الإلكترونية المتعلقة بأنظمة الدفع، تؤدي إلى فقدان المصادقية العامة في استعمال التقنيات الذكية التي تستخدمها البنوك والمصارف، نظراً للمخاطر التي تسببها نتائج ذلك الاستعمال ومنها الاعتداء على الحياة الخاصة والبرامج المعالجة آلياً عن طريق الاحتيال لارتكاب جرائم بالتقنية الذكية، مما يؤثر في زعزعة ثقة العملاء في التعاملات الرقمية في البنوك، وبسبب ما لذلك من نتائج تهدد الاقتصاد والأمن المعلوماتي لكافة البنوك، وتهديد تعامل العملاء مع هذه البنوك، لذلك عملت كافة الدول إلى سن نصوص تهدف إلى حماية كافة المعطيات والمعلومات داخل النطاق الإلكتروني من أجل كسب ثقة العملاء (الفرواني، 2022).

من جهة أخرى يرتبط نجاح المصارف والبنوك في أعمالها بمدى ثقة العملاء بعملها الذي تؤسسه كمؤسسات جديرة بالثقة، حيث أن عدم نجاح مؤسسة خدمات المدفوعات في اعتماد استراتيجية آمنة لتقديم خدمات الدفع للعملاء يؤدي إلى زعزعة الأمان والثقة لدى هؤلاء العملاء، حيث أن طبيعة المجالات المصرفية الرقمية التي تحكم أنظمة الدفع الإلكتروني ينتج عنها تهديدات أمنية سواء من ضمن المؤسسة أو خارجها، مما يسبب فقدان المصادقية لدى البنوك، حيث أن استخدام التقنيات الرقمية المتطورة في وسائل الدفع وعدم اتباع ممارسات سليمة لضمان سرية بيانات العملاء ومنع الجرائم الإلكترونية، يؤدي إلى تدهور العلاقة بين العميل والمصرف (سمير وراضية، 2022).

كما أن التحديات المتعلقة باستخدام أنظمة الدفع الإلكتروني المعتمدة لدى البنوك مرتبطة بالاختراقات الإلكترونية وعلى الرغم من التأثيرات الإيجابية لها إلا أن هناك أشكالاً متنوعة من التداعيات التي أثرت على مجموعة واسعة من الجرائم التي لم تكن معروفة من قبل لدى البنوك، لذلك انتشرت جرائم السرقة السيبرانية والسطو على حسابات البنوك وسرقتها عن طريق التعامل مع الأرقام المباشرة لهواتف العملاء، كما أن مخاطر الدفع الإلكتروني تحدث ضرراً وتؤدي إلى السيطرة على أرصدة الزبائن من خلال الثغرات الإلكترونية في منصاتها كجرائم الهجمات الإلكترونية أو التعدي غير المسموح به على برامج التشغيل، ونتيجة لذلك كان من الضروري وجود مستشعرات أجهزة تتطلب المصادقة والأمان والخصوصية، حيث تؤدي هذه الجرائم الإلكترونية إلى شعور العملاء بالقلق وانعدام الأمن وفقدان الثقة بالتعامل مع البنك (موسى و أبو بكر، 2023).

الفصل الثالث

منهجية الدراسة وإجراءاتها

أولاً- منهج الدراسة

ثانياً- مجتمع وعينة الدراسة

ثالثاً- خصائص أفراد عينة الدراسة

رابعاً- أداة الدراسة

خامساً- صدق أداة الدراسة

سادساً- أساليب المعالجة الإحصائية

الفصل الثالث

منهجية الدراسة وإجراءاتها

يتناول هذا الفصل عرضاً مفصلاً لمنهجية الدراسة الميدانية، وإجراءاتها التي استخدمت لتنفيذ الدراسة، وتحقيق أهدافها، بدءاً بتوضيح المنهج المستخدم، ومن ثم التعرف على مجتمع وعينة الدراسة وما تميزت به من خصائص، بالإضافة إلى توضيح كيفية تصميم أدلة جمع البيانات، وآلية التحقق من صدقها وثباتها، وأخيراً التطرق إلى إجراءات تطبيقها، وختم الفصل بعرض الأساليب الإحصائية المستخدمة في معالجة البيانات واستخراج النتائج، وفيما يلي عرض تفصيلي لذلك:

أولاً - منهج الدراسة:

لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها، تم استخدام المنهج الوصفي التحليلي؛ وهو كما يعرفه (العساف، ٢٠١٦، ص ٢١١) بأنه المنهج "الذي يتم بواسطة استجواب جميع مفردات مجتمع البحث أو عينة كبيرة منهم، وذلك بهدف وصف الظاهرة المدروسة من حيث طبيعتها ودرجة وجودها فقط، دون أن يتجاوز ذلك إلى دراسة العلاقة أو استنتاج الأسباب مثلاً"، والذي يعتبر من أكثر المناهج ملائمةً للدراسة الحالية، لاعتماده على وصف الواقع الحقيقي للظاهرة ومن ثم تحليل النتائج وبناء الاستنتاجات في ضوء الواقع الحالي.

ثانياً - مجتمع وعينة الدراسة:

تم أخذ عينة عشوائية بسيطة من العاملين في قطاع المدفوعات الإلكترونية مكونة من (80) مفردة، ومن المستخدمين النهائيين مكونة من (162) مفردة.

ثالثاً - خصائص أفراد الدراسة:

تم تحديد عدد من المتغيرات الرئيسية لوصف أفراد الدراسة، وتشمل: (الجنس - المستوى التعليمي - التخصص المهني - عدد سنوات الخبرة) ، والتي لها مؤشرات دلالية على نتائج الدراسة،

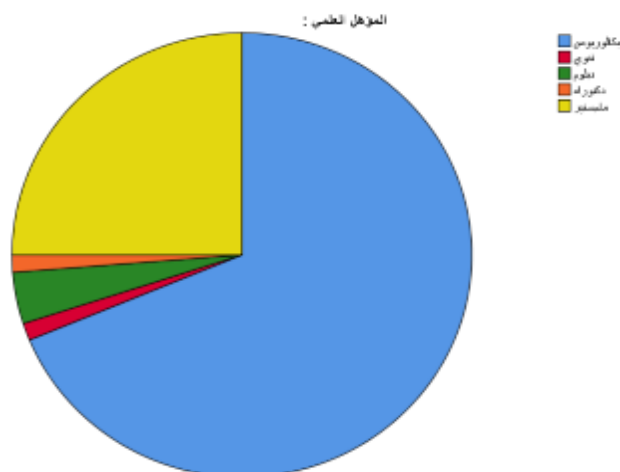
بالإضافة إلى أنها تعكس الخلفية العلمية لمفردات الدراسة، وتساعد على إرساء الدعائم التي تُبنى عليها التحليلات المختلفة المتعلقة بالدراسة، وتفصيل ذلك فيما يلي:

(١) المستوى التعليمي للعاملين :

جدول رقم (3-1) توزيع أفراد الدراسة وفق متغير المستوى التعليمي للعاملين

النسبة %	التكرار	المستوى التعليمي
68.8	55	بكالوريوس
1.3	1	ثانوي
3.8	3	دبلوم
1.3	1	دكتوراه
25.0	20	ماجستير
100%	80	المجموع

يتضح من الجدول رقم (3-1) أن (55) من أفراد الدراسة يمثلون ما نسبته 68.8% مستواهم التعليمي بكالوريوس، بينما (20) من أفراد الدراسة يمثلون ما نسبته 25.0% من إجمالي أفراد الدراسة مستواهم التعليمي ماجستير، و(3) من أفراد الدراسة يمثلون ما نسبته 3.8% من إجمالي أفراد الدراسة مستواهم التعليمي دبلوم.



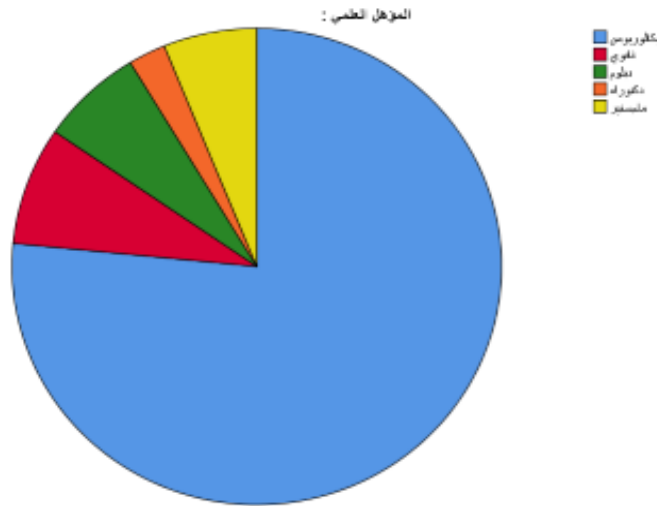
شكل رقم (3-1) توزيع أفراد الدراسة من العاملين وفق متغير المستوى التعليمي

٢) المستوى التعليمي للمستهلكين :

جدول رقم (3-2) توزيع أفراد الدراسة وفق متغير المستوى التعليمي للمستهلكين

النسبة %	التكرار	المستوى التعليمي
76.5	124	بكالوريوس
8.0	13	ثانوي
6.8	11	دبلوم
2.5	4	دكتوراه
6.2	10	ماجستير
100%	162	المجموع

يتضح من الجدول رقم (3-2) أن (124) من أفراد الدراسة يمثلون ما نسبته 76.5% مستواهم التعليمي بكالوريوس ، بينما (13) من أفراد الدراسة يمثلون ما نسبته 8.0% من إجمالي أفراد الدراسة مستواهم التعليمي ثانوي ، و(11) من أفراد الدراسة يمثلون ما نسبته 6.8% من إجمالي أفراد الدراسة مستواهم التعليمي دبلوم.



شكل رقم (3-2) توزيع أفراد الدراسة من المستهلكين وفق متغير المستوى التعليمي

٣) التخصص المهني للعاملين :

جدول رقم (3-3) توزيع أفراد الدراسة وفق متغير التخصص المهني للمستهلكين

النسبة %	التكرار	التخصص المهني
3.8	3	اعمال حرة
17.5	14	رئيس قسم
2.5	2	لا اعمل
23.8	19	مدير
8.8	7	مشرف
43.8	35	موظف
%100	80	المجموع

يتضح من الجدول رقم (3-3) أن (25) من أفراد الدراسة يمثلون ما نسبته 43.8% تخصصهم المهني موظف، بينما (19) من أفراد الدراسة يمثلون ما نسبته 23.8% من إجمالي أفراد الدراسة تخصصهم المهني مدير ، و(14) من أفراد الدراسة يمثلون ما نسبته 17.5% من إجمالي أفراد الدراسة تخصصهم المهني رئيس قسم.



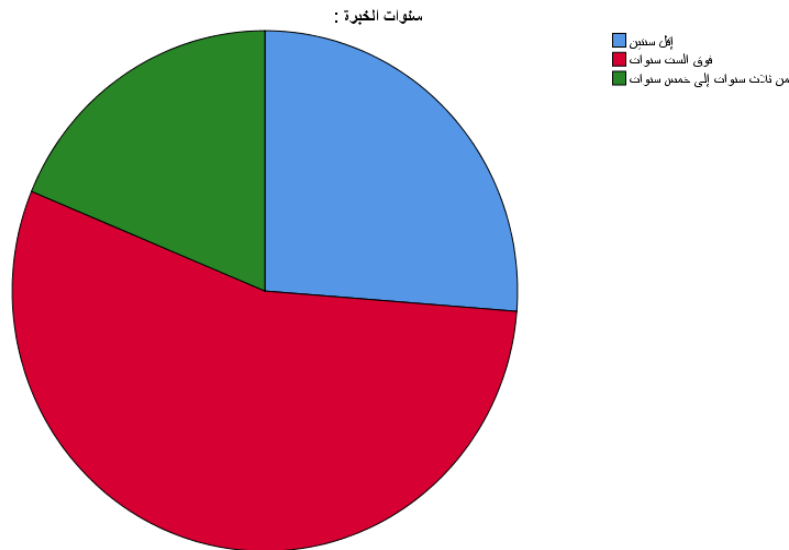
شكل رقم (3-3) توزيع أفراد الدراسة من العاملين وفق متغير التخصص المهني.

٤) عدد سنوات الخبرة للعاملين:

جدول رقم (3-4) توزيع أفراد الدراسة وفق متغير عدد سنوات الخبرة للعاملين

عدد سنوات الخبرة	التكرار	النسبة %
إقل سنتين	21	26.3
فوق الست سنوات	44	55.0
من ثلاث سنوات إلى خمس سنوات	15	18.8
المجموع	80	%100

يتضح من الجدول رقم (3-4) أن (44) من أفراد الدراسة يمثلون ما نسبته 55.0% عدد سنوات خبرتهم فوق الست سنوات ، بينما (21) من أفراد الدراسة يمثلون ما نسبته 26.3% من إجمالي أفراد الدراسة عدد سنوات خبرتهم أقل من سنتين، و(15) من أفراد الدراسة يمثلون ما نسبته 18.8% من إجمالي أفراد الدراسة عدد سنوات خبرتهم من 3 - 5 سنوات.



شكل رقم (3-4) توزيع أفراد الدراسة من العاملين وفق متغير عدد سنوات الخبرة

رابعاً- أدوات الدراسة:

تم استخدام الاستبانة لجمع البيانات من العاملين والمستهلكين؛ وذلك نظراً لمناسبتها لأهداف الدراسة، ومنهجها، ومجتمعها، وللإجابة على تساؤلاتها.

أ) بناء أدوات الدراسة:

بعد الاطلاع على الأدبيات، والدراسات السابقة ذات الصلة بموضوع الدراسة الحالية، وفي ضوء معطيات وتساؤلات الدراسة وأهدافها تم بناء الأدوات (الاستبانة)، وتكونت الاستبانة في صورتها النهائية من ثلاثة أجزاء. وفيما يلي عرض لكيفية بنائها، والإجراءات المتبعة للتحقق من صدقها، وثباتها:

١ - **القسم الأول:** يحتوي على مقدمة تعريفية بأهداف الدراسة، ونوع البيانات والمعلومات التي يود جمعها من أفراد الدراسة، مع تقديم الضمان بسرية المعلومات المقدمة، والتعهد باستخدامها لأغراض البحث العلمي فقط.

٢ - **القسم الثاني:** يحتوي على البيانات الأولية الخاصة بأفراد الدراسة، والمتمثلة في: (المستوى التعليمي - التخصص المهني - عدد سنوات الخبرة).

٣ - القسم الثالث:

_ في استمارة العاملين : يتكون من (38) عبارة، موزعة على خمسة محاور أساسية ، والجدول (3-5) يوضح عدد عبارات الاستبانة، وكيفية توزيعها على المحاور .

_ في استمارة المستهلكين : يتكون من (34) عبارة، موزعة على ستة محاور أساسية ، والجدول (3-6) يوضح عدد عبارات الاستبانة، وكيفية توزيعها على المحاور .

جدول (3-5) محاور استبانة العاملين وعباراتها

عدد العبارات	المحور
5	خدمات الدفع الإلكتروني التي يستعملها العملاء في المملكة العربية السعودية من وجهة نظر العاملين
6	المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر العاملين
10	العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني من وجهة نظر العاملين
8	مخاطر الدفع الإلكتروني وعلاقته بالجرائم الإلكترونية
9	التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم
38 عبارة	الاستبانة

جدول (3-6) محاور استبانة المستهلكين وعباراتها

عدد العبارات	المحور
5	خدمات الدفع الإلكتروني التي يستخدمها العملاء في المملكة العربية السعودية من وجهة نظر المستهلكين
5	المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر المستهلكين
5	العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني من وجهة نظر المستهلكين
7	تأثير مخاطر خدمات الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة
6	وعي المستهلكين بمخاطر وسائل الدفع الإلكتروني لمنع حدوث الجرائم
6	التدابير التي يمكن أن يتبعها المستهلك للحد من هذه المخاطر والجرائم
34 عبارة	الاستبانة

تم استخدام مقياس ليكرت الخماسي للحصول على استجابات أفراد الدراسة، وفق درجات الموافقة التالية: (أوافق بشدة - أوافق - محايد - غير موافق - غير موافق بشدة)، ومن ثم التعبير عن هذا المقياس كمياً، بإعطاء كل عبارة من العبارات السابقة درجة، وفقاً للتالي: أوافق بشدة (5) درجات، أوافق (4) درجات، محايد (3) درجات، غير موافق (2) درجتان، غير موافق بشدة (1) درجة واحدة. ولتحديد طول فئات مقياس ليكرت الخماسي، تم حساب المدى بطرح الحد الأعلى من الحد الأدنى (5-1 = 4)، ثم تم تقسيمه على أكبر قيمة في المقياس (4 ÷ 5 = 0.80)، وبعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس (1)؛ لتحديد الحد الأعلى لهذه الفئة، وهكذا أصبح طول الفئات كما هو موضح في الجدول التالي:

جدول (3-7) تقسيم فئات مقياس ليكرت الخماسي (حدود متوسطات الاستجابات)

م	الفئة	حدود الفئة		مقياس الحكم
		من	إلى	
1	غير موافق بشدة	1.00	1.80	منخفض جداً
2	غير موافق	1.81	2.60	منخفض
3	محايد	2.61	3.40	متوسط
4	أوافق	3.41	4.20	مرتفع
5	أوافق بشدة	4.21	5.00	مرتفع جداً

وتم استخدام طول المدى في الحصول على حكم موضوعي على متوسطات استجابات أفراد الدراسة، بعد معالجتها إحصائياً.

خامساً- صدق أدوات الدراسة:

صدق أداة الدراسة يعني التأكد من أنها تقيس ما أعدت كما يقصد به شمول الأدوات لكل العناصر التي تدخل في التحليل من ناحية، ووضوح عباراتها من ناحية أخرى، بحيث تكون مفهومة لكل من يستخدمها وقد تم التأكد من صدق أدوات الدراسة من خلال:

١- الصدق الظاهري لأدوات الدراسة :

للتعرف على مدى الصدق الظاهري للأدوات، والتأكد من أنها تقيس ما وضعت لقياسه، عُرضت بصورتها الأولية على المشرف، وبعد أخذ الآراء، والاطلاع على الملاحظات، أُجريت التعديلات اللازمة التي اتفق عليها، ومن ثم أُخرجت الأدوات بصورتها النهائية (ملحق رقم 1 و2).

٢- صدق الاتساق الداخلي للاستبانة :

للتحقق من صدق الاتساق الداخلي للاستبانة، حُسِبَ معامل ارتباط بيرسون (Pearson's Correlation Coefficient)؛ للتعرف على درجة ارتباط كل عبارة من عبارات الاستبانة الموجهة للعاملين وللمستهلكين بالدرجة الكلية للمحور .

الجدول رقم (3-8) معاملات ارتباط بيرسون لعبارات المحاور مع الدرجة الكلية للمحور الخاصة باستبانة العاملين

رقم المحور والعبارة	معامل الارتباط بالمحور	رقم المحور والعبارة	معامل الارتباط بالمحور
المحور الأول ع1	**0.702	المحور الثالث ع9	**0.760
المحور الأول ع2	**0.780	المحور الثالث ع10	**0.668
المحور الأول ع3	**0.759	المحور الرابع ع1	**0.566
المحور الأول ع4	**0.752	المحور الرابع ع2	**0.761
المحور الأول ع5	**0.789	المحور الرابع ع3	**0.841
المحور الثاني ع1	**0.650	المحور الرابع ع4	**0.564
المحور الثاني ع2	**0.754	المحور الرابع ع5	**0.605
المحور الثاني ع3	**0.716	المحور الرابع ع6	**0.851
المحور الثاني ع4	**0.669	المحور الرابع ع7	**0.843
المحور الثاني ع5	**0.705	المحور الرابع ع8	**0.713
المحور الثاني ع6	**0.666	المحور الخامس ع1	**0.764
المحور الثالث ع1	**0.576	المحور الخامس ع2	**0.730
المحور الثالث ع2	**0.773	المحور الخامس ع3	**0.820

معامل الارتباط بالمحور	رقم المحور والعبارة	معامل الارتباط بالمحور	رقم المحور والعبارة
**0.820	المحور الخامس ع4	**0.689	المحور الثالث ع3
**0.710	المحور الخامس ع5	**0.753	المحور الثالث ع4
**0.839	المحور الخامس ع6	**0.779	المحور الثالث ع5
**0.746	المحور الخامس ع7	**0.815	المحور الثالث ع6
**0.560	المحور الخامس ع8	**0.486	المحور الثالث ع7
**0.675	المحور الخامس ع9	**0.641	المحور الثالث ع8

**** دال عند مستوى الدلالة 0.01 فأقل**

يتضح من الجدول (3 - 8) أن قيم معامل ارتباط كل عبارة من العبارات مع محورها موجبة، ودالة إحصائياً عند مستوى الدلالة (0.01) فأقل؛ مما يشير إلى صدق الاتساق الداخلي بين عبارات المحور الأول، ومناسبتها لقياس ما أعدت لقياسه. كما تم حساب معامل ارتباط بيرسون (Pearson's Correlation Coefficient)؛ للتعرف على درجة ارتباط كل محور من المحاور بالدرجة الكلية للاستبانة وتوضح الجداول التالية معاملات الارتباط.

الجدول رقم (3 - 9) معاملات ارتباط بيرسون للمحاور مع الدرجة الكلية للاستبانة الموجهة للعاملين

معامل الارتباط بالاستبانة	المحور
**0.572	خدمات الدفع الإلكتروني التي يستخدمها العملاء في المملكة العربية السعودية
**0.625	المخاطر المرتبطة بخدمات الدفع الإلكتروني
**0.850	العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني
**0.759	مخاطر الدفع الإلكتروني وعلاقته بالجرائم الإلكترونية
**0.875	التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم

**** دال عند مستوى الدلالة 0.01 فأقل**

يتضح من الجدول (3 - 9) أن قيم معامل ارتباط كل محور مع الاستبانة موجبة، ودالة إحصائياً عند مستوى الدلالة (0.01) فأقل؛ مما يشير إلى صدق الاتساق الداخلي بين المحاور، ومناسبتها لقياس ما أعدت لقياسه.

الجدول رقم (3-10) معاملات ارتباط بيرسون لعبارات المحاور مع الدرجة الكلية للمحور الخاصة باستبانة

المستهلكين

معامل الارتباط بالمحور	رقم المحور والعبارة	معامل الارتباط بالمحور	رقم المحور والعبارة
**0.613	المحور الرابع ع3	**0.785	المحور الأول ع1
**0.554	المحور الرابع ع4	**0.679	المحور الأول ع2
**0.789	المحور الرابع ع5	**0.443	المحور الأول ع3
**0.741	المحور الرابع ع6	**0.773	المحور الأول ع4
**0.265	المحور الرابع ع7	**0.767	المحور الأول ع5
**0.606	المحور الخامس ع1	**0.683	المحور الثاني ع1
**0.504	المحور الخامس ع2	**0.796	المحور الثاني ع2
**0.487	المحور الخامس ع3	**0.812	المحور الثاني ع3
**0.531	المحور الخامس ع4	**0.813	المحور الثاني ع4
**0.795	المحور الخامس ع5	**0.568	المحور الثاني ع5
**0.694	المحور الخامس ع6	**0.775	المحور الثالث ع1
**0.642	المحور السادس ع1	**0.739	المحور الثالث ع2
**0.730	المحور السادس ع2	**0.767	المحور الثالث ع3
**0.779	المحور السادس ع3	**0.774	المحور الثالث ع4
**0.730	المحور السادس ع4	**0.692	المحور الثالث ع5
**0.789	المحور السادس ع5	**0.266	المحور الرابع ع1
**0.806	المحور السادس ع6	**0.651	المحور الرابع ع2

** دال عند مستوى الدلالة 0.01 فأقل

يتضح من الجدول (3 - 10) أن قيم معامل ارتباط كل عبارة من العبارات مع محورها موجبة، ودالة إحصائياً عند مستوى الدلالة (0.01) فأقل؛ مما يشير إلى صدق الاتساق الداخلي بين عبارات المحور الأول، ومناسبتها لقياس ما أعدت لقياسه.

كما تم حساب معامل ارتباط بيرسون (Pearson's Correlation Coefficient)؛ للتعرف على درجة ارتباط كل محور من المحاور بالدرجة الكلية للاستبانة وتوضح الجداول التالية معاملات الارتباط.

الجدول رقم (3 - 11) معاملات ارتباط بيرسون للمحاور مع الدرجة الكلية للاستبانة

الموجهة للعاملين

المحور	معامل الارتباط بالاستبانة
خدمات الدفع الإلكتروني التي يستخدمها العملاء في المملكة العربية السعودية	0.642**
المخاطر المرتبطة بخدمات الدفع الإلكتروني	0.730**
العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني	0.779**
تأثير مخاطر خدمات الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة	0.730**
وعي المستهلكين بمخاطر وسائل الدفع الإلكتروني لمنع حدوث الجرائم	0.789**
التدابير التي يمكن أن يتبعها المستهلك للحد من هذه المخاطر والجرائم	0.806**

** دال عند مستوى الدلالة 0.01 فأقل

يتضح من الجدول (3 - 11) أن قيم معامل ارتباط كل محور مع الاستبانة موجبة، ودالة إحصائياً عند مستوى الدلالة (0.01) فأقل؛ مما يشير إلى صدق الاتساق الداخلي بين المحاور، ومناسبتها لقياس ما أعدت لقياسه.

(ب) ثبات أداة الدراسة:

تم التأكد من ثبات أداة الدراسة من خلال استخدام معامل الثبات ألفا كرونباخ (معادلة ألفا كرونباخ) (α Cronbach's Alpha)، ومعادلة التجزئة النصفية (Split-half)، ويوضح الجدول رقم (3-12) والجدول (3 - 13) قيم معاملات الثبات ألفا كرونباخ لكل محور من محاور الاستبانة الموجهة للعاملين والمستهلكين على الترتيب.

جدول رقم (3-12) معامل ألفا كرونباخ والتجزئة النصفية (Split-half) لقياس ثبات أداة الدراسة الموجهة

للعاملين

الاستبانة	عدد العبارات	ألفا كرونباخ	التجزئة النصفية
خدمات الدفع الإلكتروني التي يستخدمها العملاء في المملكة العربية السعودية	5	0.810	0.803
المخاطر المرتبطة بخدمات الدفع الإلكتروني	6	0.783	0.781
العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني	10	0.866	0.813
مخاطر الدفع الإلكتروني وعلاقته بالجرائم الإلكترونية	8	0.865	0.864
التدابير التي يمكن أن تتبناها المنظمة للحد من هذه المخاطر والجرائم	9	0.888	0.848
الثبات العام	38	0.931	0.814

يتضح من الجدول رقم (3-12) أن معامل الثبات العام عالٍ حيث بلغ (0.931) وفق معادلة كرونباخ ألفا، بينما بلغ في التجزئة النصفية (0.814)، وهذا يدل على أن الاستبانة تتمتع بدرجة ثبات مرتفعة يمكن الاعتماد عليها في التطبيق الميداني للدراسة.

جدول رقم (3-13) معامل ألفا كرونباخ والتجزئة النصفية (Split-half) لقياس ثبات أداة الدراسة الموجهة للمستهلكين

التجزئة النصفية	ألفا كرونباخ	عدد العبارات	الاستبانة
0.728	0.732	5	خدمات الدفع الإلكتروني التي يستخدمها العملاء في المملكة العربية السعودية
0.662	0.786	5	المخاطر المرتبطة بخدمات الدفع الإلكتروني
0.674	0.799	5	العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني
0.656	0.655	7	تأثير مخاطر خدمات الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة
0.522	0.652	6	وعي المستهلكين بمخاطر وسائل الدفع الإلكتروني لمنع حدوث الجرائم
0.788	0.833	6	التدابير التي يمكن أن يتبعها المستهلك للحد من هذه المخاطر والجرائم
0.724	0.834	34	الثبات العام

يتضح من الجدول رقم (3-13) أن معامل الثبات العام عالٍ حيث بلغ (0.834) وفق معادلة كرونباخ ألفا، بينما بلغ في التجزئة النصفية (0.724)، وهذا يدل على أن الاستبانة تتمتع بدرجة ثبات مرتفعة يمكن الاعتماد عليها في التطبيق الميداني للدراسة.

إجراءات تطبيق الدراسة:

بعد التأكد من صدق (الاستبانة) وثباتها، وصلاحياتها للتطبيق، تم تطبيقها ميدانياً باتباع الخطوات التالية:

١- توزيع الأدوات إلكترونياً.

٢- جمع الأدوات، وقد بلغ عددها (80) استبانة للعاملين، و (162) استبانة للمستهلكين.

سادساً- أساليب المعالجة الإحصائية:

لتحقيق أهداف الدراسة، وتحليل البيانات التي تم تجميعها، فقد تم استخدام العديد من الأساليب الإحصائية المناسبة باستخدام الحزم الإحصائية للعلوم الاجتماعية Statistical Package for Social Sciences والتي يرمز لها اختصاراً بالرمز (SPSS).

وبعد ذلك تم حساب المقاييس الإحصائية التالية:

- ١ - التكرارات، والنسب المئوية؛ للتعرف على خصائص أفراد الدراسة، وتحديد استجاباتهم تجاه عبارات المحاور الرئيسة التي تتضمنها أداة الدراسة.
- ٢ - المتوسط الحسابي الموزون (المرجح) "Weighted Mean"؛ وذلك للتعرف على متوسط استجابات أفراد الدراسة على كل عبارة من عبارات المحاور، كما أنه يفيد في ترتيب العبارات حسب أعلى متوسط حسابي موزون.
- ٣ - المتوسط الحسابي "Mean"؛ وذلك لمعرفة مدى ارتفاع، أو انخفاض استجابات أفراد الدراسة عن المحاور الرئيسة، مع العلم بأنه يفيد في ترتيب المحاور حسب أعلى متوسط حسابي.
- ٤ - الانحراف المعياري "Standard Deviation"؛ للتعرف على مدى انحراف استجابات أفراد الدراسة لكل عبارة من عبارات متغيرات الدراسة، ولكل محور من المحاور الرئيسة عن متوسطها الحسابي. ويلاحظ أن الانحراف المعياري يوضح التشتت في استجابات أفراد الدراسة لكل عبارة من عبارات متغيرات الدراسة، إلى جانب المحاور الرئيسة، فكلما اقتربت قيمته من الصفر تركزت الاستجابات، وانخفض تشتتها.
- ٥ - تم استخدام معامل ارتباط بيرسون للتحقق من صدق الاتساق الداخلي لأداة الدراسة.
- ٦ - تم استخدام معامل الفا كرونباخ للتحقق من ثبات أداة الدراسة.
- ٧ - تم استخدام معادلة التجزئة النصفية للتحقق من ثبات أداة الدراسة.

الفصل الرابع

تحليل نتائج الدراسة وتفسيرها

أولاً- تحليل نتائج الاستبيان الموجه للعاملين

ثانياً- تحليل نتائج الاستبيان الموجه للمستهلكين

الفصل الرابع

تحليل نتائج الدراسة وتفسيرها

يتناول هذا الفصل عرضاً تفصيلياً للنتائج التي توصلت إليها الدراسة الحالية، وذلك من خلال الإجابة عن أسئلة الدراسة وفق المعالجات الإحصائية المناسبة، ومن ثم تفسير هذه النتائج، وذلك على النحو التالي:

أولاً- تحليل بيانات الاستبيان الموجه للعاملين:

المحور الأول: ما هي خدمات الدفع الإلكتروني من وجهة نظر العاملين؟

للتعرف على خدمات الدفع الإلكتروني من وجهة نظر العاملين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور ، وجاءت النتائج كما يلي:

جدول رقم (4 - 1) استجابات أفراد الدراسة من العاملين حول خدمات الدفع الإلكتروني مرتبة تنازلياً حسب

متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الترتيب	الدرجة / الحكم
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
1	يستخدم العملاء خدمات الدفع الإلكتروني بشكل يومي ومتكرر	ك	58	19	3	-	-	4.68	0.541	أوافق بشدة	1	مرتفع جداً
		%	72.5	23.8	3.8	-	-					
2	يستخدم العملاء خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات	ك	58	16	6	-	-	4.65	0.635	أوافق بشدة	2	مرتفع جداً
		%	72.5	20	7.5	-	-					
4	يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول أو البطاقات	ك	53	23	3	1	-	4.60	0.628	أوافق بشدة	3	مرتفع جداً
		%	66.3	28.7	3.8	1.3	-					
3	يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية	ك	31	20	1	1	1	4.57	0.742	أوافق بشدة	4	مرتفع جداً
		%	57.4	37	1.9	1.9	1.9					

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	درجة	الدرجة / التقييم
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
	الشراء عبر الإنترنت من المواقع الإلكترونية											
5	يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية تحويل الأموال عبر المحافظ وإجراء المعاملات المالية و شحن الرصيد	ك	49	26	5	-	-	4.55	0.614	أوافق بشدة	5	مرتفع جداً
		%	61.3	32.5	6.3	-	-					
	المتوسط العام											
								4.61	0.830	أوافق بشدة		مرتفع جداً

يتضح في الجدول (4-1) أن هناك درجة مرتفعة جداً حول خدمات الدفع الإلكتروني بمتوسط حسابي بلغ (4.61 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة على أداة الدراسة.

ويتضح من النتائج في الجدول (4-1) أن أبرز الاستجابات تتمثل في العبارات رقم (1، 2، 4) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (1) وهي: "يستخدم العملاء خدمات الدفع الإلكتروني بشكل يومي ومتكرر" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.68 من 5.00).

٢ - جاءت العبارة رقم (2) وهي: "يستخدم العملاء خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.65 من 5.00).

٣ - جاءت العبارة رقم (4) وهي: "يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول أو البطاقات" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.60 من 5.00).

المحور الثاني: ما هي المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر العاملين؟

للتعرف على المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر العاملين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 2) استجابات أفراد الدراسة من العاملين حول المخاطر المرتبطة بخدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الرتبة	الدرجة / الحكم
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
1	خدمات الدفع الإلكتروني تحمل مخاطر عالية تتعلق بالاختراقات الأمنية	ك	33	31	10	4	2	4.11	0.890	أوافق بشدة	1	مرتفع جداً
		%	41.2	38.4	12.5	5	2					
3	استخدام خدمات الدفع الإلكتروني تعرض العميل للاختيال المالي	ك	26	30	18	6	-	3.95	0.926	أوافق	2	مرتفع
		%	32.5	37.3	22.5	7.5	-					
5	هناك خطراً من إساءة استخدام معلومات العميل من قبل بعض موظفي الشركات المقدمة لخدمات الدفع الإلكتروني	ك	21	31	20	6	2	3.78	1.002	أوافق	3	مرتفع
		%	26.3	38.8	25	7.5	2.5					
6	هناك نقصاً في الدعم والمساعدة الفورية في حالة تعرض العميل لمشكلات أمنية أثناء استخدام خدمات الدفع الإلكتروني	ك	25	18	10	-	1	3.77	1.078	أوافق	4	مرتفع
		%	46.3	33.3	18.5	-	1.9					
4	هناك احتمالية كبيرة لفقدان بيانات العميل الشخصية عند استخدام خدمات الدفع الإلكتروني	ك	19	27	20	12	2	3.61	1.084	أوافق	5	مرتفع
		%	23.8	33.8	25	15	2					
2	خدمات الدفع الإلكتروني تساهم في زيادة مخاطر غسل الأموال وتمويل الإرهاب	ك	25	16	11	1	1	3.58	1.121	أوافق	6	مرتفع
		%	46.3	29.6	20.4	1.9	1.9					

الدرجة / المقياس	الفئة	الانحراف المعياري	المتوسط الحسابي	درجة الموافقة					التكرار	العبارات	م
				غير موافق بشدة	غير موافق	محايد	أوافق	أوافق بشدة			
مرتفع جداً	أوافق بشدة	0.915	4.56	المتوسط العام							

يتضح في الجدول (4-2) أن هناك درجة مرتفعة حول المخاطر المرتبطة بخدمات الدفع الإلكتروني بمتوسط حسابي بلغ (4.56 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 4.20) ، وهي الفئة التي تشير إلى خيار أوافق بشدة على أدلة الدراسة. ويتضح من النتائج في الجدول (4-2) أن أبرز الاستجابات تتمثل في العبارات رقم (1، 3، 5) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (1) وهي: "خدمات الدفع الإلكتروني تحمل مخاطر عالية تتعلق بالاختراقات الأمنية" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (4.11 من 5.00).

٢ - جاءت العبارة رقم (3) وهي: "تنوع الآلات والأجهزة ساعد على إتمام المهام المطلوبة" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (3.95 من 5.00).

٣ - جاءت العبارة رقم (5) وهي: "هناك خطراً من إساءة استخدام معلومات العميل من قبل بعض موظفي الشركات المقدمة لخدمات الدفع الإلكتروني" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (3.78 من 5.00).

نجد مما سبق بأن نتائج الدراسة الحالية تتفق مع نتائج دراسة طالة لامية (2022) والتي توصلت إلى أن هناك عدة مخاطر أمنية يمكن أن تتعرض لها المعاملات التجارية عند استخدام النقود الإلكترونية، مثل الاحتيال وسرقة البيانات والاختراقات الإلكترونية، كما أنها تتفق مع دراسة سبيحي سمير (2021) والتي أكدت إلى أن أبرز التحديات الأمنية التي تواجه المستخدمين تتمثل في الاحتيال، القرصنة، وسرقة البيانات الشخصية.

تحليل المحور الثالث: ما هي العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني من وجهة نظر العاملين؟

للتعرف على العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني من وجهة نظر العاملين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 3) استجابات أفراد الدراسة من العاملين حول العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الترتيب	الرتبة / الترتيب
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
10	توعية العملاء بأهمية اتباع ممارسات الأمان عند استخدام خدمات الدفع الإلكتروني وعدم مشاركة معلوماتهم الشخصية مع الآخرين	ك	65	12	2	1	-	4.76	0.556	أوافق بشدة	1	مرتفع جداً
		%	81.3	15	2.5	1.3	-					
4	تشفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها	ك	53	22	3	1	-	4.65	0.827	أوافق بشدة	2	مرتفع جداً
		%	50	40.7	5.6	1.9	-					
5	استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية	ك	26	45	4	-	-	4.65	0.597	أوافق بشدة	3	مرتفع جداً
		%	48.1	42.6	7.4	-	-					
6	التحديث المستمر للبرامج والنظم	ك	50	13	8	1	1	4.61	0.754	أوافق بشدة	4	مرتفع جداً
		%	57.4	24.1	14.8	1.3	1.3					
3	تجريم جميع الأفعال التي فيها مساس بالأنظمة الإلكترونية ومستخدميها	ك	42	27	8	-	-	4.57	0.745	أوافق بشدة	5	مرتفع جداً
		%	53.7	27.8	14.8	-	-					
9	الالتزام بفحص صحة عمليات الدفع الإلكتروني من خلال الإستعانة بالتقنيات الحديثة	ك	60	17	7	1	1	4.57	0.726	أوافق بشدة	6	مرتفع جداً
		%	51.9	31.5	11.1	1.3	1.3					
1	ربط وسائل الدفع الإلكتروني بوسائل أمان تساعد في تحديد هوية العملاء	ك	56	22	7	1	-	4.56	0.894	أوافق بشدة	7	مرتفع جداً
		%	48.1	35.2	13	1.9	-					

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الدرجة	الدرجة / المقياس
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
2	استخدام أساليب متقدمة للمصادقة	ك	24	17	10	2	-	4.56	0.972	أوافق بشدة	8	مرتفع جداً
		%	44.4	31.5	.18	2.5	-					
7	الاحتفاظ بنسخ احتياطية للبيانات الموجودة	ك	48	19	9	2	2	4.36	0.723	أوافق بشدة	9	مرتفع جداً
		%	60	23.8	11.3	2.5	2.5					
8	استخدام جهاز قارئ للبطاقة يقوم بقراءة معلومات وسائل الدفع الإلكتروني	ك	36	23	13	7	1	4.07	0.957	أوافق بشدة	10	مرتفع جداً
		%	45	28.7	16.3	8.8	1.3					
	المتوسط العام											
								4.53	0.734	أوافق بشدة		مرتفع جداً

يتضح في الجدول (3-4) أن هناك درجة مرتفعة جداً حول العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني بمتوسط حسابي بلغ (4.53 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة على أداة الدراسة.

ويتضح من النتائج في الجدول (3-4) أن أبرز الاستجابات تتمثل في العبارات رقم (10، 4، 5) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (10) وهي: "توعية العملاء بأهمية اتباع ممارسات الأمان عند استخدام خدمات الدفع الإلكتروني وعدم مشاركة معلوماتهم الشخصية مع الآخرين" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.76 من 5.00).

٢ - جاءت العبارة رقم (4) وهي: "شفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.65 من 5.00).

٣ - جاءت العبارة رقم (5) وهي "استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.65 من 5.00).

تتفق نتائج هذه الدراسة مع دراسة فلاح الفليح (2021) والتي وجدت إلى أن هناك مسؤولية مدنية تقع على عاتق مزودي خدمات الدفع الإلكتروني تجاه العملاء في حال حدوث أي خلل أو تقصير في تقديم الخدمات، بالإضافة إلى أنهم يتوجب عليهم حماية حقوق المستهلكين وضمان أمن المعاملات الإلكترونية.

المحور الرابع: ماهي العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي من وجهة نظر العاملين ؟

للتعرف على العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي من وجهة نظر العاملين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا، وجاءت النتائج كما يلي:

جدول رقم (4 - 4) استجابات أفراد الدراسة من العاملين حول العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الترتيب	الدرجة / الحكم
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
4	عدم وجود إجراءات واضحة للتبليغ عن الجرائم المالية قد يمكن المجرمين من العمل دون أن يتم اكتشافهم بسرعة	ك	57	21	2	-	-	4.68	0.517	أوافق بشدة	1	مرتفع جداً
		%	71.3	26.3	2.5	-	-					
3	عدم توفير التدريب المناسب للموظفين حول كيفية التعامل مع الجرائم المالية والتهديدات الأمنية يمكن أن يترك الشركة عرضة للمخاطر	ك	57	18	4	1	-	4.62	0.700	أوافق بشدة	2	مرتفع جداً
		%	71.3	22.5	5	1.3	-					
5	الاعتماد على تقنيات قديمة أو غير محدثة قد يجعل الأنظمة عرضة للاختراقات والهجمات الإلكترونية	ك	57	18	4	1	-	4.62	0.700	أوافق بشدة	3	مرتفع جداً
		%	71.3	22.5	5	1.3	-					
6	عدم وجود سياسات صارمة لإدارة المخاطر المالية والأمنية قد يجعل من الصعب اكتشاف	ك	55	19	4	1	1	4.57	0.759	أوافق بشدة	4	مرتفع جداً
		%	68.8	23.8	5	1.3	1.3					

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	رتبة	الدرجة / الرتبة
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
	ومواجهة الاحتيال والجرائم المالية											
7	عدم فرض رقابة صارمة على من يتمتعون بصلاحيات الوصول إلى البيانات والأنظمة يمكن أن يؤدي إلى الوصول غير المصرح به واستخدامه بشكل غير قانوني	ك	25	38	32	47	20	4.52	0.745	أوافق بشدة	5	مرتفع جداً
		%	15.4	23.5	19.8	29	12.3					
2	عدم إجراء مراجعات دورية ومنظمة للحسابات والنظم قد يمكن للمحتالين من استغلال الثغرات والضعف في النظام	ك	48	26	3	1	2	4.46	0.841	أوافق بشدة	6	مرتفع جداً
		%	60	32.5	3.8	1.3	2.5					
8	عدم السرعة في التعامل مع الشكاوي والمشكلات الأمنية التي تواجه العميل أثناء استخدام خدمات الدفع الإلكتروني	ك	33	29	19	55	26	4.45	0.870	أوافق بشدة	7	مرتفع جداً
		%	20.4	17.9	11.7	34	16					
1	عدم القيام بفحص كافٍ للعملاء قد يؤدي إلى استخدام الحسابات بطرق غير مشروعة أو لأنشطة غير قانونية	ك	41	30	6	3	-	4.36	0.783	أوافق بشدة	8	مرتفع جداً
		%	51.2	37.5	7.5	3.8	-					
	المتوسط العام							4.53	0.830	أوافق بشدة		مرتفع جداً

يتضح في الجدول (4-4) أن هناك درجة مرتفعة جداً حول العلاقة بين مخاطر الدفع الإلكتروني وحدوث الجرائم الإلكترونية في السوق السعودي بمتوسط حسابي بلغ (4.53 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة. ويتضح من النتائج في الجدول (4-4) أن أبرز الاستجابات تتمثل في العبارات رقم (4، 3، 5) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (4) وهي: "عدم وجود إجراءات واضحة للتبليغ عن الجرائم المالية قد يمكن المجرمين من العمل دون أن يتم اكتشافهم بسرعة" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.68 من 5.00).

٢ - جاءت العبارة رقم (3) وهي: "عدم توفير التدريب المناسب للموظفين حول كيفية التعامل مع الجرائم المالية والتهديدات الأمنية يمكن أن يترك الشركة" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.62 من 5.00).

٣ - جاءت العبارة رقم (5) وهي "الاعتماد على تقنيات قديمة أو غير محدثة قد يجعل الأنظمة عرضة للاختراقات والهجمات الإلكترونية" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.62 من 5.00).

المحور الخامس: ماهي التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم من وجهة نظر العاملين؟

للتعرف على التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم من وجهة نظر العاملين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 5) استجابات أفراد الدراسة من العاملين حول التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	النسبة	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	ترتيب	الدرجة / التكرار
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
1	التحقق من مخاطر العميل قبل الدخول معه في علاقة عمل والربط مع جهات حكومية موثوقة للتحقق من هوية العميل	ك	57	21	1	1	-	4.67	0.556	أوافق بشدة	1	مرتفع جداً
		%	71.3	26.3	1.3	1.3	-					
9	فرض قيود جغرافية على المعاملات المالية، بحيث يتم قبول المعاملات فقط ضمن	ك	53	22	3	1	-	4.67	0.611	أوافق بشدة	2	مرتفع جداً
		%	50	40.7	5.6	1.9	-					

م	العبارة	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الدرجة	الدرجة / المقياس
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
	مناطق محددة ومعروفة مسبقاً، مما يساعد في تقليل فرص الاحتيال والجرائم المالية											
2	استخدام بروتوكول أمن بين المستخدم والخادم المالي، يستخدم طبقة تشفير لحماية البيانات المرسلة والمستقبلية	ك	55	23	2	-	-	4.63	0.621	أوافق بشدة	3	مرتفع جداً
		%	68.8	28.7	2.5	-	-					
5	الاستفادة من خبرات الخبراء في أمن المعلومات يمكن أن تسهم في تعزيز أمان خدمات الدفع الإلكتروني	ك	50	13	8	1	1	4.62	0.754	أوافق بشدة	4	مرتفع جداً
		%	57.4	24.1	14.8	1.3	1.3					
4	الاستثمار في تحديث التقنيات وتطوير البنية التحتية	ك	55	20	8	1	1	4.58	0.745	أوافق بشدة	5	مرتفع جداً
		%	68.8	25	14.8	1.3	1.3					
6	التحليلات البيانية والذكاء الاصطناعي يساهم في التنبؤ بالتهديدات الأمنية	ك	60	17	7	1	1	4.58	0.726	أوافق بشدة	6	مرتفع جداً
		%	51.9	31.5	11.1	1.3	1.3					
3	استخدام توثيق متعدد العوامل لتأكيد هوية المستخدم في عملية الدفع الإلكتروني	ك	52	20	4	-	4	4.50	0.894	أوافق بشدة	7	مرتفع جداً
		%	65	25	5	-	5					
7	وجود تعاون بين مختلف الأطراف في قطاع خدمات الدفع الإلكتروني يساهم في تعزيز الأمان والحد من الجرائم الإلكترونية	ك	47	25	6	1	1	4.45	0.972	أوافق بشدة	8	مرتفع جداً
		%	58.8	31.5	7.5	1.3	1.3					
8	تنظيم دورات تدريبية وتوعية العاملين بانتظام حول كيفية اكتشاف ومنع الجرائم المالية، بما في ذلك التعرف على أساليب الاحتيال الشائعة والإجراءات الأمنية اللازمة لحماية المعلومات المالية	ك	44	20	12	1	3	4.28	0.723	أوافق بشدة	9	مرتفع جداً
		%	55	25	15	1.3	3.8					

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الدرجة	الدرجة / المقياس
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
			المتوسط العام					4.55	0.829	أوافق بشدة	مرتفع جداً	

يتضح في الجدول (4-5) أن هناك درجة مرتفعة جداً حول التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم بمتوسط حسابي بلغ (4.55 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة.

ويتضح من النتائج في الجدول (4-5) أن أبرز الاستجابات تتمثل في العبارات رقم (1، 9، 2) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (1) وهي: "التحقق من مخاطر العميل قبل الدخول معه في علاقة عمل والربط مع جهات حكومية موثوقة للتحقق من هوية العميل " بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.67 من 5.00).

٢ - جاءت العبارة رقم (9) وهي: " فرض قيود جغرافية على المعاملات المالية، بحيث يتم قبول المعاملات فقط ضمن مناطق محددة ومعروفة مسبقاً، مما يساعد في تقليل فرص الاحتيال والجرائم المالية " بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.67 من 5.00).

٣ - جاءت العبارة رقم (2) وهي " استخدام بروتوكول آمن بين المستخدم والخادم المالي، يستخدم طبقة تشفير لحماية البيانات المرسل والمستقبل " بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.63 من 5.00).

تتفق نتائج هذه الدراسة مع دراسة بوليد لعماري (2019) التي أكدت بأن هناك عدة مخاطر غدا استخدام وسائل الدفع الإلكتروني، لذلك لابد من وجود ضمانات قانونية لمواجهة هذه المخاطر والحد من انتشارها وتفاقم وقوعها.

ثانياً - تحليل بيانات الاستبيان الموجه للمستهلكين:

المحور الأول: ما هي خدمات الدفع الإلكتروني من وجهة نظر المستهلكين؟
للتعرف على خدمات الدفع الإلكتروني من وجهة نظر المستهلكين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور ، وجاءت النتائج كما يلي:

جدول رقم (4 - 6) استجابات أفراد الدراسة من المستهلكين حول خدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الترتبة	الدرجة / التكرار
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
2	أستخدم خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات	ك	110	39	7	4	2	4.54	0.796	أوافق بشدة	1	مرتفع جداً
		%	72.5	23.8	3.8	2.5	1.2					
4	أستخدم خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول أو البطاقات الائتمانية	ك	101	43	10	5	3	4.44	0.884	أوافق بشدة	2	مرتفع جداً
		%	62.5	26	7.5	3.1	1.9					
5	أستخدم خدمات الدفع الإلكتروني لإمكانية تحويل الأموال عبر المحافظ وإجراء المعاملات المالية وشحن الرصيد	ك	96	52	13	6	2	4.43	0.869	أوافق بشدة	3	مرتفع جداً
		%	59.3	32.1	11.3	3.7	1.9					
3	أستخدم خدمات الدفع الإلكتروني لإمكانية الشراء عبر الإنترنت من المواقع الإلكترونية	ك	88	52	19	2	1	4.38	0.789	أوافق بشدة	4	مرتفع جداً
		%	54	32.4	11.7	1.2	1.6					
1	أستخدم خدمات الدفع الإلكتروني بشكل يومي ومتكرر الرصيد	ك	87	46	16	13	-	4.27	0.940	أوافق بشدة	5	مرتفع جداً
		%	53.7	28.4	9.9	8	-					
	المتوسط العام											
								4.41	0.988	أوافق بشدة		مرتفع جداً

يتضح في الجدول (4-6) أن هناك درجة مرتفعة جداً حول خدمات الدفع الإلكتروني بمتوسط حسابي بلغ (4.41 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00)، وهي الفئة التي تشير إلى خيار أوافق بشدة على أدلة الدراسة.

ويتضح من النتائج في الجدول (4-6) أن أبرز الاستجابات تتمثل في العبارات رقم (2، 4، 5) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (2) وهي: "أستخدم خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.54 من 5.00).

٢ - جاءت العبارة رقم (4) وهي: "أستخدم خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول أو البطاقات الائتمانية" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.44 من 5.00).

٣ - جاءت العبارة رقم (5) وهي: "أستخدم خدمات الدفع الإلكتروني لإمكانية تحويل الأموال عبر المحافظ وإجراء المعاملات المالية وشحن الرصيد" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.43 من 5.00).

وتتفق نتائج هذه الدراسة مع دراسة عبد الرحمن الجهمي وأحمد شهاب (2023) عن مدى سهولة استخدام الخدمات الإلكترونية المقدمة من المنشآت السعودية للمستهلكين، الأمر الذي يشجع العملاء على استمرار استخدام خدمات الدفع الإلكترونية لإمكانية تسديد الفواتير والاشتراكات فضلاً عن إجراء المعاملات المالية.

المحور الثاني: ما هي المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر المستهلكين؟

للتعرف على المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر المستهلكين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 7) استجابات أفراد الدراسة من المستهلكين حول المخاطر المرتبطة بخدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الترتيب	الدرجة / التقييم
			النسبة	أوافق بشدة	أوافق	محايد	غير موافق					
1	تحميل خدمات الدفع الإلكتروني مخاطر عالية تتعلق بالاختراقات الأمنية	ك	110	39	7	4	2	4.04	0.957	أوافق	1	مرتفع
		%	72.5	23.8	3.8	2.5	1.2					
2	استخدام خدمات الدفع الإلكتروني يمكن أن يعرضني للاحتيال المالي	ك	101	43	10	5	3	4.00	0.884	أوافق	2	مرتفع
		%	62.5	26	7.5	3.1	1.9					
4	هناك خطرًا من إساءة استخدام معلوماتي من قبل موظفي الشركات المقدمة لخدمات الدفع الإلكتروني	ك	96	52	13	6	2	3.84	0.869	أوافق	3	مرتفع
		%	59.3	32.1	11.3	3.7	1.9					
3	هناك احتمالية كبيرة لفقدان بياناتي الشخصية عند استخدام خدمات الدفع الإلكتروني	ك	88	52	19	2	1	3.72	1.023	أوافق	4	مرتفع
		%	54	32.4	11.7	1.2	1.6					
5	هناك نقصًا في الدعم والمساعدة الفورية في حالة تعرضي لمشكلات أمنية أثناء استخدام خدمات الدفع الإلكتروني	ك	87	46	16	13	-	3.69	1.024	أوافق	5	مرتفع
		%	53.7	28.4	9.9	8	-					
المتوسط العام												
								3.85	1.021	أوافق		مرتفع

يتضح في الجدول (4-7) أن هناك درجة مرتفعة حول المخاطر المرتبطة بخدمات الدفع الإلكتروني بمتوسط حسابي بلغ (3.85 من 5.00) ، وهو متوسط يقع في الفئة الرابعة من فئات المقياس الخماسي (من 3.41 إلى 4.20) ، وهي الفئة التي تشير إلى خيار أوافق على أداة الدراسة.

ويتضح من النتائج في الجدول (4-7) أن أبرز الاستجابات تتمثل في العبارات رقم (1، 2، 4) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (1) وهي: "تحميل خدمات الدفع الإلكتروني مخاطر عالية تتعلق بالاختراقات الأمنية" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (4.04 من 5.00).

٢ - جاءت العبارة رقم (2) وهي: "استخدام خدمات الدفع الإلكتروني يمكن أن يعرضني للاحتيال المالي بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (4.00 من 5.00).

٣ - جاءت العبارة رقم (4) وهي: "هناك خطراً من إساءة استخدام معلوماتي من قبل موظفي الشركات المقدمة لخدمات الدفع الإلكتروني" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (3.84 من 5.00).

تتفق نتائج هذه الدراسة مع دراسة مي خريسات (2022) التي هدفت إلى التعرف على إيجابيات وسلبيات الدفع الإلكتروني في المملكة العربية السعودية، والتي توصلت إلى أن هناك عدد من السلبيات للدفع الإلكتروني لا بد من الوقوف عندها والعمل على إيجاد الحلول المناسبة لها.

تحليل المحور الثالث: ما هي العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني من وجهة نظر المستهلكين؟

للتعرف على العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني من وجهة نظر المستهلكين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 8) استجابات أفراد الدراسة من المستهلكين حول العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	النسبة	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	ترتيب	الدرجة / الترتيب
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
4	تشفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها	ك	135	20	6	1	-	4.78	0.957	أوافق بشدة	1	مرتفع جداً
		%	83.5	12.3	3.7	0.6	-					
3	تجريم جميع الأفعال التي فيها مساس بالأنظمة الإلكترونية ومستخدميها	ك	126	29	5	1	1	4.71	0.615	أوافق بشدة	2	مرتفع جداً
		%	77.8	17.9	3.1	0.6	0.6					
5		ك	123	28	9	1	1	4.67	0.667		3	

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الرتبة	الدرجة / الحكم
			النسبة	أوافق بشدة	أوافق	محايد	غير موافق					
	استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية	%	75	17.3	5.6	0.6				أوافق بشدة		مرتفع جداً
2	استخدام أساليب متقدمة للمصادقة	ك	115	40	6	1	-	4.66	1.023	أوافق بشدة	4	مرتفع جداً
		%	71	24.7	3.7	0.6	-					
1	ربط وسائل الدفع الإلكتروني بوسائل أمان تساعد في تحديد هوية العملاء	ك	116	34	8	3	1	4.61	1.024	أوافق بشدة	5	مرتفع جداً
		%	71.6	21	4.9	1.9	0.6					
المتوسط العام												
								4.68	0.918	أوافق بشدة		مرتفع جداً

يتضح في الجدول (4-8) أن هناك درجة مرتفعة جداً حول العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني بمتوسط حسابي بلغ (4.68 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة على أدلة الدراسة.

ويتضح من النتائج في الجدول (4-8) أن أبرز الاستجابات تتمثل في العبارات رقم (4، 3، 5) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (4) وهي: "تشفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.78 من 5.00).

٢ - جاءت العبارة رقم (3) وهي: "تجريم جميع الأفعال التي فيها مساس بالأنظمة الإلكترونية ومستخدميها" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.71 من 5.00).

٣ - جاءت العبارة رقم (5) وهي "استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.67 من 5.00).

المحور الرابع: ما هو تأثير مخاطر الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة؟

للتعرف على تأثير مخاطر الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 9) استجابات أفراد الدراسة حول تأثير مخاطر الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الترتيب	الدرجة / الترتيب
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
1	تقدم البنوك والمؤسسات المالية في المملكة مستوى عالٍ من الحماية لمستخدمي خدمات الدفع الإلكتروني	ك	52	62	31	13	4	3.89	1.025	أوافق	1	مرتفع
		%	32.1	38.3	19.1	8	2.5					
4	المخاطر المرتبطة بخدمات الدفع الإلكتروني تؤثر على قراري باستخدامها في المعاملات المالية الكبيرة	ك	52	59	30	13	8	3.82	1.117	أوافق	2	مرتفع
		%	32.1	36.4	18.5	8	4.9					
7	خدمات الدعم الفني المتاحة تساعدني في التعامل مع المشكلات الأمنية عند استخدام خدمات الدفع الإلكتروني	ك	35	61	51	13	2	3.70	0.938	أوافق	3	مرتفع
		%	21.6	37.7	31.5	8	1.2					
3	من الممكن اختراق حساباتي عند استخدام خدمات الدفع الإلكتروني	ك	34	32	12	1	-	3.62	1.023	أوافق	4	مرتفع
		%	71	24.7	3.7	0.6	-					
5	أفضل استخدام النقد أو وسائل الدفع التقليدية بسبب المخاوف الأمنية من الدفع الإلكتروني	ك	25	38	32	47	20	3.00	1.282	محايد	5	متوسط
		%	15.4	23.5	19.8	29	12.3					
2		ك	33	29	19	55	26	2.92	1.407	محايد	6	متوسط

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الترتبة	الدرجة / الحكم
			النسبة	أوافق بشدة	أوافق	محايد	غير موافق					
	تعرضت لجرائم إلكترونية مرتبطة بخدمات الدفع الإلكتروني	%	20.4	17.9	11.7	34	16					
6	أنا على استعداد لدفع رسوم إضافية مع السداد عند الاستلام عوضاً عن الدفع الإلكتروني بسبب قلقي من مخاطر الدفع الإلكتروني	ك	27	23	26	58	28	2.77	1.347	محايد	7	متوسط
	%	16.7	14.2	16	35.8	17.3						
	المتوسط العام					3.38	0.830	أوافق	مرتفع			

يتضح في الجدول (4-9) أن هناك درجة مرتفعة جداً حول تأثير مخاطر الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة بمتوسط حسابي بلغ (3.83 من 5.00) ، وهو متوسط يقع في الفئة الرابعة من فئات المقياس الخماسي (من 3.41 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة على أداة الدراسة.

ويتضح من النتائج في الجدول (4-9) أن أبرز الاستجابات تتمثل في العبارات رقم (1، 4، 7) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (1) وهي: "تقدم البنوك والمؤسسات المالية في المملكة مستوى عالٍ من الحماية لمستخدمي خدمات الدفع الإلكتروني" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (3.89 من 5.00).

٢ - جاءت العبارة رقم (4) وهي: "المخاطر المرتبطة بخدمات الدفع الإلكتروني تؤثر على قراري باستخدامها في المعاملات المالية الكبيرة" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (3.82 من 5.00).

٣ - جاءت العبارة رقم (7) وهي "خدمات الدعم الفني المتاحة تساعدني في التعامل مع المشكلات الأمنية عند استخدام خدمات الدفع الإلكتروني" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها وبدرجة مرتفعة بمتوسط حسابي بلغ (3.70 من 5.00).

بناءً على ما سبق نجد أن نتائج هذه الدراسة تتفق مع نتائج دراسة سفر (2008) والتي أكدت بأن التحديات التي تواجه خدمات الدفع الإلكتروني والتي تتمثل بقضايا الأمان وانتهاك الخصوصية ممكن أن تؤثر على قرار اعتماد هذه الخدمات.

تحليل المحور الخامس: ماهي العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي من وجهة نظر المستهلكين؟

للتعرف على العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي من وجهة نظر المستهلكين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 10) استجابات أفراد الدراسة من المستهلكين حول العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	رتبة	الترتيب / الم
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
3	أفضل تلقي تنبيهات فورية عندما يتم استخدام حسابي أو بطاقتي لعمليات دفع غير معتادة أو غير مصرح بها	ك	135	21	5	-	1	4.78	0.554	أوافق بشدة	1	مرتفع جداً
		%	83.3	13	3.1	-	0.6					
4	أفضل استخدام خدمات الدفع الإلكتروني التي توفر تقنيات تحقق إضافية مثل الرموز السرية أو التحقق الفئائي لتعزيز الأمان	ك	127	31	3	1	-	4.75	0.511	أوافق بشدة	2	مرتفع جداً
		%	62.5	26	7.5	0.6	-					
1	تحقق دائماً من صحة المواقع والتطبيقات التي تستخدمها للدفع الإلكتروني قبل إدخال بياناتك المالية	ك	98	54	7	2	1	4.51	0.698	أوافق بشدة	3	مرتفع جداً
		%	60.5	33.3	4.3	1.2	0.6					
2	تقديم معلوماتك المالية عبر الإنترنت يمكن أن يتعرض لخطر الاختراق أو الاستخدام غير المصرح به	ك	88	52	19	1	1	4.40	0.735	أوافق بشدة	4	مرتفع جداً
		%	54	32.4	11.7	0.6	0.6					

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الدرجة	الدرجة / المقياس
		النسبة	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
5	أقوم بتحديث برامج الحماية المضادة للفيروسات بانتظام لحماية جهازي من البرمجيات الخبيثة التي قد تحدد معلوماتي المالية عند استخدام الدفع الإلكتروني	ك	77	35	28	17	5	4.00	1.163	أوافق	5	مرتفع
		%	47.5	21.6	17.3	10.5	3.1					
6	أشارك في التدريبات أو الدورات التي تعزز من وعي بأمان الدفع الإلكتروني وكيفية حماية معلوماتي المالية عبر إنترنت	ك	40	40	49	27	6	3.50	1.143	أوافق	6	مرتفع
		%	24.7	24.7	30.2	16.7	3.7					
المتوسط العام												
								4.32	0.830	أوافق بشدة		مرتفع جداً

يتضح في الجدول (4-10) أن هناك درجة مرتفعة جداً حول العلاقة بين مخاطر الدفع الإلكتروني وحدوث الجرائم الإلكترونية في السوق السعودي بمتوسط حسابي بلغ (4.32 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة على أداة الدراسة.

ويتضح من النتائج في الجدول (4-10) أن أبرز الاستجابات تتمثل في العبارات رقم (3، 4، 1) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (3) وهي: "أفضل تلقي تنبيهات فورية عندما يتم استخدام حسابي أو بطاقتي لعمليات دفع غير معتادة أو غير مصرح بها" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.78 من 5.00).

٢ - جاءت العبارة رقم (4) وهي: "أفضل استخدام خدمات الدفع الإلكتروني التي توفر تقنيات تحقق إضافية مثل الرموز السرية أو التحقق الثنائي لتعزيز الأمان" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.75 من 5.00).

٣- جاءت العبارة رقم (1) وهي "تحقق دائماً من صحة المواقع والتطبيقات التي تستخدمها للدفع الإلكتروني قبل إدخال بياناتك المالية" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.51 من 5.00).

تحليل المحور السادس: ماهي التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم من وجهة نظر المستهلكين؟

للتعرف على التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم من وجهة نظر المستهلكين، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على عبارات هذا المحور، وجاءت النتائج كما يلي:

جدول رقم (4 - 11) استجابات أفراد الدراسة من المستهلكين حول التدابير التي يمكن أن تتبعها المنظمة للحد من

هذه المخاطر والجرائم مرتبة تنازلياً حسب متوسطات الموافقة

م	العبارات	النسبة	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	ترتيب	الدرجة / التكرار
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
2	التصريح الفوري حال ضياع البطاقة الإلكترونية أو فقدانها	ك	130	27	4	1	-	4.76	0.517	أوافق بشدة	1	مرتفع جداً
		%	80.2	16.7	2.5	0.6	-					
4	اعتماد تطبيقات ومواقع الدفع الآمنة	ك	126	31	4	1	-	4.73	0.566	أوافق بشدة	2	مرتفع جداً
		%	77.8	19.1	2.5	0.6	-					
1	استخدام كلمات سر قوية	ك	109	48	2	3	1	4.62	0.610	أوافق بشدة	3	مرتفع جداً
		%	67.3	29.6	1.2	1.9	0.6					
3	التحقق الدوري من الحسابات المالية لاكتشاف أي نشاط غير طبيعي او مشبوه	ك	104	31	4	1	-	4.58	0.627	أوافق بشدة	4	مرتفع جداً
		%	64.2	19.3	2.5	0.6	-					
5	متابعة أحدث المستجدات والممارسات الأمنية في مجال الدفع الإلكتروني	ك	88	52	19	2	1	4.38	0.789	أوافق بشدة	5	مرتفع جداً
		%	54.3	32.1	11.7	1.2	0.6					
6	تحديث نظام التشغيل، المتصفح، وبرامج الحماية من الفيروسات بشكل دوري	ك	89	50	16	4	3	4.34	0.893	أوافق بشدة	6	مرتفع جداً
		%	54.9	30.9	9.9	2.5	1.9					

م	العبارات	التكرار	درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	الفئة	الدرجة	الدرجة / المقياس
			أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة					
			المتوسط العام					4.56	0.830	أوافق بشدة	مرتفع جداً	

يتضح في الجدول (4-11) أن هناك درجة مرتفعة جداً حول التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم بمتوسط حسابي بلغ (4.56 من 5.00) ، وهو متوسط يقع في الفئة الخامسة من فئات المقياس الخماسي (من 4.21 إلى 5.00) ، وهي الفئة التي تشير إلى خيار أوافق بشدة على أداة الدراسة.

ويتضح من النتائج في الجدول (4-11) أن الاستجابات تتمثل في العبارات رقم (2، 4، 1) التي تم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً، كالتالي:

١ - جاءت العبارة رقم (2) وهي: "التصريح الفوري حال ضياع البطاقة الإلكترونية أو فقدانها" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.76 من 5.00).

٢ - جاءت العبارة رقم (4) وهي: "اعتماد تطبيقات ومواقع الدفع الآمنة" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.73 من 5.00).

٣ - جاءت العبارة رقم (1) وهي "استخدام كلمات سر قوية" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بشدة وبدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.62 من 5.00).

الفصل الخامس

خلاصة نتائج الدراسة وتوصياتها ومقترحاتها

أولاً- خلاصة الدراسة

ثانياً- أهم نتائج الدراسة

ثالثاً- توصيات الدراسة

رابعاً- مقترحات الدراسة

الفصل الخامس

خلاصة نتائج الدراسة وتوصياتها ومقترحاتها

يحتوي هذا الفصل على ملخص الدراسة، وأبرز ما توصلت إليه من نتائج، يليها عرض لأهم التوصيات في ضوء تلك النتائج، وختاماً تمت الإشارة إلى جملة من المقترحات لدراسات مستقبلية.

أولاً- خلاصة الدراسة:

ضمت الدراسة في طياتها خمسة فصول، بالإضافة إلى قائمة المراجع والملاحق، وذلك على النحو التالي:

الفصل الأول، ويشمل: مقدمة الدراسة، ومشكلتها، وأسئلتها، وأهدافها، وأهميتها، والدراسات السابقة وحدودها، وأهم مصطلحاتها.

الفصل الثاني، ويشمل الإطار النظري.

الفصل الثالث، ويشمل: منهجية الدراسة وإجراءاتها، حيث تم استخدام المنهج الوصفي المسحي، والاستبانة أداة للدراسة. كما تم في هذا الفصل توضيح لكيفية بناء الاستبانة، وآلية التحقق من صدقها وثباتها، وإجراءات تطبيق الدراسة، والأساليب الإحصائية المستخدمة في معالجة البيانات.

الفصل الرابع، ويشمل: عرضاً مفصلاً لنتائج الدراسة، وتحليلها، وتفسيرها؛ من أجل الوصول إلى أهداف الدراسة، وذلك بالإجابة عن أسئلة الدراسة.

الفصل الخامس، ويشمل: ملخص الدراسة، وأبرز ما انتهت إليه من نتائج، والتوصيات المقترحة في ضوء تلك النتائج، والمقترحات لدراسات مستقبلية.

ثانياً- أهم نتائج الدراسة:

توصلت الدراسة إلى عددٍ من النتائج، ومن أبرزها:

إجابة السؤال الأول: ما هي خدمات الدفع الإلكتروني؟

هناك درجة مرتفعة من الآراء حول خدمات الدفع الإلكتروني.

أبرز الاستجابات حول هذا المحور من وجهة نظر العاملين تتمثل في:

١- يستخدم العملاء خدمات الدفع الإلكتروني بشكل يومي ومتكرر.

- ٢- يستخدم العملاء خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات.
- ٣- يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول أو البطاقات.

أبرز الاستجابات حول هذا المحور من وجهة نظر المستهلكين تتمثل في:

- ١- أستخدم خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات.
- ٢- أستخدم خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول أو البطاقات الائتمانية.
- ٣- أستخدم خدمات الدفع الإلكتروني لإمكانية تحويل الأموال عبر المحافظ وإجراء المعاملات المالية وشحن الرصيد.

إجابة السؤال الثاني: ما هي المخاطر المرتبطة بخدمات الدفع الإلكتروني؟

هناك درجة مرتفعة من الآراء حول المخاطر المرتبطة بخدمات الدفع الإلكتروني.

أبرز الاستجابات حول هذا المحور من وجهة نظر العاملين تتمثل في:

- ١- خدمات الدفع الإلكتروني تحمل مخاطر عالية تتعلق بالاختراقات الأمنية.
- ٢- استخدام خدمات الدفع الإلكتروني تعرض العميل للاحتيال المالي.
- ٣- هناك خطرًا من إساءة استخدام معلومات العميل من قبل بعض موظفي الشركات المقدمة لخدمات الدفع الإلكتروني.

أبرز الاستجابات حول هذا المحور من وجهة نظر المستهلكين تتمثل في:

- ١- تحمل خدمات الدفع الإلكتروني مخاطر عالية تتعلق بالاختراقات الأمنية.
- ٢- استخدام خدمات الدفع الإلكتروني يمكن أن يعرضني للاحتيال المالي.
- ٣- هناك خطرًا من إساءة استخدام معلوماتي من قبل موظفي الشركات المقدمة لخدمات الدفع الإلكتروني.

إجابة السؤال الثالث: ما هي العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني؟

هناك درجة مرتفعة من الآراء حول العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني.

أبرز الاستجابات حول هذا المحور من وجهة نظر العاملين تتمثل في:

1- توعية العملاء بأهمية اتباع ممارسات الأمان عند استخدام خدمات الدفع الإلكتروني وعدم مشاركة معلوماتهم الشخصية مع الآخرين

2- تشفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها

3- استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية

أبرز الاستجابات حول هذا المحور من وجهة نظر المستهلكين تتمثل في:

1- تشفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها

2- تجريم جميع الأفعال التي فيها مساس بالأنظمة الإلكترونية ومستخدميها

٤ - استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية.

إجابة السؤال الخامس: ماهو تأثير مخاطر الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة؟

هناك درجة مرتفعة من الآراء حول تأثير مخاطر الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة.

أبرز الاستجابات حول هذا المحور من وجهة نظر المستهلكين تتمثل في:

١- تقدم البنوك والمؤسسات المالية في المملكة مستوى عالٍ من الحماية لمستخدمي خدمات الدفع الإلكتروني.

٢- المخاطر المرتبطة بخدمات الدفع الإلكتروني تؤثر على قراري باستخدامها في المعاملات المالية الكبيرة.

٣- خدمات الدعم الفني المتاحة تساعدني في التعامل مع المشكلات الأمنية عند استخدام خدمات الدفع الإلكتروني.

إجابة السؤال السادس: ماهي العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي؟

هناك درجة مرتفعة من الآراء حول العلاقة بين مخاطر الدفع الإلكتروني وحوادث الجرائم الإلكترونية في السوق السعودي.

أبرز الاستجابات حول هذا المحور من وجهة نظر العاملين تتمثل في:

١- عدم وجود إجراءات واضحة للتبليغ عن الجرائم المالية قد يمكن المجرمين من العمل دون أن يتم اكتشافهم بسرعة.

٢- عدم توفير التدريب المناسب للموظفين حول كيفية التعامل مع الجرائم المالية والتهديدات الأمنية يمكن أن يترك الشركة عرضة للمخاطر.

٣- الاعتماد على تقنيات قديمة أو غير محدثة قد يجعل الأنظمة عرضة للاختراقات والهجمات الإلكترونية.

أبرز الاستجابات حول هذا المحور من وجهة نظر المستهلكين تتمثل في:

1- أفضل تلقي تنبيهات فورية عندما يتم استخدام حسابي أو بطاقتي لعمليات دفع غير معتادة أو غير مصرح بها.

2- أفضل استخدام خدمات الدفع الإلكتروني التي توفر تقنيات تحقق إضافية مثل الرموز السرية أو التحقق الثنائي لتعزيز الأمان.

٤- تحقق دائماً من صحة المواقع والتطبيقات التي تستخدمها للدفع الإلكتروني قبل إدخال بياناتك المالية.

إجابة السؤال السابع: ماهي التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم؟ هناك درجة مرتفعة من الآراء حول التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم.

أبرز الاستجابات حول هذا المحور من وجهة نظر العاملين تتمثل في:

١- التحقق من هوية العميل قبل الدخول معه في علاقة عمل والربط مع جهات حكومية موثوقة للتحقق من هوية العميل

٢- فرض قيود جغرافية على المعاملات المالية، بحيث يتم قبول المعاملات فقط ضمن مناطق محددة ومعروفة مسبقاً، مما يساعد في تقليل فرص الاحتيال والجرائم المالية

٣- استخدام بروتوكول آمن بين المستخدم والخادم المالي، يستخدم طبقة تشفير لحماية البيانات المرسل والمستقبل

أبرز الاستجابات حول هذا المحور من وجهة نظر المستهلكين تتمثل في:

١- التصريح الفوري حال ضياع البطاقة الإلكترونية أو فقدانها.

٢ - اعتماد تطبيقات ومواقع الدفع الآمنة.

٣ - استخدام كلمات سر قوية.

ثالثاً- توصيات الدراسة:

في ضوء النتائج التي تم التوصل إليها، فإن الدراسة توصي بما يلي:

- ضرورة نشر الثقافة الإلكترونية من خلال برامج التوعية حول مخاطر أنظمة الدفع الإلكتروني .

- ضرورة اعتماد التوقيع الإلكتروني لتجنب حدوث الجرائم الإلكترونية.

- ضرورة تشفير البيانات المتعلقة بحسابات العملاء .

- توعية العملاء بمخاطر مشاركة البيانات والمعلومات الشخصية على مواقع التواصل الاجتماعي.

- العمل على بناء قاعدة قانونية وتشريعية صارمة تجاه الجرائم الإلكترونية.

- التطوير والتحديث المستمر لأنظمة الرقابة البنكية والتحقق من فعاليتها.

- ضرورة الرقابة الداخلية على عمل الموظفين داخل البنوك أو مؤسسات خدمات المدفوعات.

- نشر الوعي بأهمية التبليغ الفوري عن ضياع البطاقات البنكية.

- استعمال تقنيات عالية الجودة تعيق اختراقات قرصنة الإنترنت.

- ضرورة الاحتفاظ بنسخ احتياطية من الأنظمة والبرامج الإلكترونية ضمن خطة للطوارئ.

- تطوير أداء العاملين في مؤسسات خدمات المدفوعات، وتدريبهم بشكل دوري.

- توفير الضوابط اللازمة للرقابة على المعلومات الخاصة بمعاملات الدفع الإلكتروني.

- مراجعة السياسات والإجراءات المرتبطة بمعاملات الدفع الإلكتروني بشكل منتظم.

- ضرورة رفع مستوى الخدمات البنكية الإلكترونية.

- ضرورة توفير الدعم المادي لتطوير شبكة الاتصالات.

- تطبيق استراتيجيات تدعم انتشار خدمات أنظمة الدفع الإلكتروني بشكل آمن.

رابعاً- المقترحات:

- إجراء دراسات مستقبلية حول التحديات التي تواجه فعالية أنظمة الدفع الإلكترونية
- إجراء دراسات مستقبلية حول طرق انتشار الجرائم الإلكترونية.
- إجراء دراسات مستقبلية حول شخصية وأهداف قراصنة الإنترنت والدوافع التي تقف وراء ارتكابهم للاختراقات والجرائم الإلكترونية.

قائمة المصادر والمراجع:

- أحسن، رابحي. (2009). الجريمة الإلكترونية النقطة المظلمة بالنسبة للتكنولوجيا المعلوماتية، جامعة بوفرة بومرداس، مجلة دراسات وأبحاث، مج 1، ع1.
- إدارة البحوث والتنمية. (2019). وسائل الدفع الإلكتروني الأشهر والأوسع نطاقاً، مجلة اتحاد المصارف العربية، اتحاد المصارف العربية، العدد 460.
- أسماء، برنيس؛ حسنى، تيلاني. (2019). دور نظم الدفع الإلكتروني في تحقيق رضى الزبون دراسة حالة بنك الفلاحة والتنمية الريفية وكالة ميله، رسالة ماجستير، الجزائر.
- الأمين، زهير الصائم. (2014). الدفع الآلي مستقبل الخدمات المصرفية 2-2، مجلة المال والاقتصاد، العدد 76.
- باشا، كريمة أحمد شايب. (2020). وسائل الدفع الإلكتروني: مخاطرها وتحديات الحماية منها، مجلة الوقائع القانونية، مجلد 1، العدد 4.
- بركات، عزت (2000). ظاهرة غسل الأموال وآثارها الاقتصادية والاجتماعية. جامعة الزرقاء الأهلية، الأردن.
- بريكة، السعيد. (2014). تحديات وسائل الدفع الإلكتروني: دراسة استطلاعية من وجهة نظر الموظفين بالوكالات البنكية لولاية أم البواقي، مجلة البحوث الاقتصادية والمالية، جامعة العربي بن مهيدي أم البواقي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، العدد الثاني.
- بلطرش، ربيعة؛ مشتر، فاطمة. (2017). مدخل عام حول وسائل الدفع الإلكتروني، الملتقى الوطني الثامن حول " آليات تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري يومي 13 و14 مارس 2017، جامعة أكلي محند أولحاج البويرة، كلية العلوم الاقتصادية والتجارية وعلوم التسيير.
- بلو ميديا للتقنية وتكنولوجيا المعلومات (2023). حلول الدفع الإلكتروني: تسهيل المعاملات التجارية في السعودية.
- البنك المركزي السعودي (2022). حصة المدفوعات الإلكترونية تتجاوز مستهدف برنامج تطوير القطاع المالي لعام 2021م .
- بوادي، مصطفى. (2017). الدفع الإلكتروني كآلية لحماية المستهلك ومظاهر تطبيقه في التشريع الجزائري، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، مخبر أثر الاجتهاد القضائي على حركة التشريع، العدد 14.

- التميمي، فراس (2023)، دور الدفع الإلكتروني في الحد من جريمة غسل الأموال. مركز النهرين الدراسات الاستراتيجية .
- الجهيمي، عبد الرحمن و د.أحمد، شهاب (2023) . الخدمات الإلكترونية وأثرها على المستهلكين في المملكة العربية السعودية. دراسة ميدانية .المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، مصر، 4 (13 ،) 101 – 120
- خبازي، فاطمة الزهرة.(2017). جرائم الدفع الإلكتروني وسبل مكافحتها، أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي وجامعة تلمسان، كلية العلوم الاقتصادية، مخبر الحوكمة العمومية والاقتصاد الاجتماعي.
- خريسات، مي (2022) . إيجابيات وسلبيات الدفع الإلكتروني في المؤسسات الحكومية. المجلة العربية للنشر العلمي . العدد واحد وأربعون .
- خليفة، محمد. (د.ت). خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري، كلية الآداب والعلوم الاجتماعية، جامعة قالم، مجلة دراسات وأبحاث.
- العكاليك، حمزة (2024)، تحديات الاحتيال ومكافحة غسل الأموال في التكنولوجيا المالية. وكالة سرايا الإخبارية .
- طالة، لامية (2022). النقود الإلكترونية: بين تسهيل أنظمة الدفع الإلكتروني ومخاطرها على أمن المعاملات التجارية. مجلة الاستاذ الباحث للدراسات القانونية والسياسية -المجلد 66 - العدد 61 - جوان 26.
- لعماري، وليد (2019). الضمانات القانونية ضد مخاطر استخدام وسائل الدفع الإلكتروني. كلية الحقوق .جامعة الجزائر .
- ذهيبية، محمد (2018). مخاطر الدفع الإلكتروني عبر الإنترنت التي يتعرض لها المستهلك الإلكتروني وإستراتيجية الجزائر لحمايته: مشروع التصديق والتوقيع الإلكترونيين .
- راشد، الطيب. (2018). الجرائم الإلكترونية الواقعة على الأموال في القانون التونسي، المؤتمر التاسع لرؤساء المحاكم العليا، بيروت.
- الربيعي، نورهان محمد. (2024). الجريمة الإلكترونية وآليات مكافحتها، كلية الحقوق، جامعة عجمان، الإمارات العربية المتحدة، مجلة الفارابي للعلوم الإنسانية، ع1، مج3.
- رضا، ثافان عبد العزيز. (2023). وسائل الدفع والوفاء الإلكترونية، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، كلية القانون والعلوم السياسية، مجلد 12، العدد 45.

- رميسة، نجوش؛ شريفة، بلقاسمي. (2018). دور أنظمة وسائل الدفع الإلكترونية في تحسين الخدمات المصرفية دراسة حالة البنك الخارجي الجزائري BEA وكالة تبسة-46، رسالة ماجستير، علوم تجارية.
- سدخان، سناء محمد. (2020). نظام الدفع والتحصيل الإلكتروني لنفقات الدولة وإيراداتها، مجلة الفكر القانوني والسياسي، جامعة عمار ثلجي الأغواط، كلية الحقوق والعلوم السياسية، المجلد 4، العدد 1.
- سفر، أحمد (2008). أنظمة الدفع الإلكتروني. لبنان، منشورات الحلبي الحقوقية.
- سمير، سبيحي (2021). مخاطر الدفع الإلكتروني. جامعة لونيبي علي البليدة - الجزائر. مجلة البحوث والدراسات القانونية والسياسية. السنة 12 المجلد 11 / العدد 02
- شاهين، علي عبد الله. (2010). نظم الدفع الإلكترونية ومخاطرها ووسائل الرقابة عليها (دراسة تطبيقية على بنك فلسطين)، مجلة جامعة الأزهر بغزة، سلسلة العلوم الإنسانية، المجلد 12، العدد 1.
- الشبول، شاكر أحمد. (2023). الحماية الجنائية لوسائل الدفع الإلكتروني: دراسة مقارنة، مجلة جرش للبحوث والدراسات، المجلد 24، العدد 2.
- صقر، رواد مليود. (2020). الحماية الأمنية لأنظمة لدفع الإلكتروني، سلسلة المعارف القانونية والقضائية، مج 74.
- الطفيلي، محمد حمزة يوسف. (2023). أثر وسائل الدفع الإلكتروني على بعض متغيرات الاقتصاد الكلي تجارب دول مختارة مع الإشارة للعراق، رسالة ماجستير، كلية الإدارة والاقتصاد، جامعة كربلاء.
- عائشة، نايري. (2017). الجريمة الإلكترونية في التشريع الجزائري، رسالة ماجستير في القانون الإداري، جامعة أحمد دراية ادرار، كلية الحقوق والعلوم السياسية.
- عبد الله، عبد الله عبد الكريم. (2011). جرائم المعلوماتية والإنترنت - الجرائم الإلكترونية، بيروت، منشورات الحلبي الحقوقية.
- العجمي، عبد الله دغش. (2014). المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط.
- عسيري، علي (2023). المملكة تسجل أعلى معدل في تبني المدفوعات عبر تقنية الاتصال قريب المدى، وكالة الأنباء السعودية.

- العساف، صالح أحمد. (٢٠١٦). المدخل إلى البحث في العلوم السلوكية، ط٣، الرياض، دار الزهراء للنشر والتوزيع.
- العفيفي، يوسف خليل يوسف. (2013). الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير، الجامعة الإسلامية، غزة.
- الفرواني، جواد. (2022). الجرائم الذكية بين النص القانوني والعمل القضائي، مجلة القانون والأعمال، جامعة الحسن الأول.
- الفليح، فلاح (2021) . المسؤولية المدنية لمزود خدمات الدفع الإلكتروني، جامعة الشرق الأوسط
- القادري، مولاي حفيظ العلوي. (2018). وسائل الدفع والأداء الإلكتروني، المجلة المغربية للاقتصاد والقانون المقارن، جامعة القاضي عياض، كلية العلوم القانونية والاقتصادية والاجتماعية، العدد 57.
- قرومي، حميد. (2014). واقع وسائل الدفع الإلكتروني في الجزائر، مجلة دراسات اقتصادية، مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، العدد 24.
- قيرة، سعاد. (2022). واقع وسائل الدفع الإلكتروني في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، مج 15، ع4.
- كنزة، راشدي؛ عائشة، راشدي. (2022). دور نظام الدفع الإلكتروني في ظل المخاطر المالية دراسة حالة BNP من 2016 إلى 2020، رسالة ماجستير، جامعة ابن خلدون تيارت.
- كنه، هبا. (2022). واقع تطبيق أنظمة الدفع الإلكتروني وأثرها في الأداء المصرفي دراسة ميدانية على بنك بيمو السعودي الفرنسي في سوريا، رسالة ماجستير، إدارة أعمال.
- محمودي، سماح. (2023). آليات مواجهة المخاطر القانونية المترتبة عن استخدام وسائل الدفع الإلكتروني، مجلة طبية للدراسات العلمية الأكاديمية، المركز الجامعي سي الحواس بريكة، مجلد 4، العدد 3.
- مرعي، إسراء جبريل رشاد. (2016). الجرائم الإلكترونية الأهداف والأسباب ومعالجتها، المركز الديمقراطي العربي للدراسات الاستراتيجية الاقتصادية والسياسية.
- مشري، فريد؛ قاجة، أمنة. (2018). الحماية القانونية لوسائل الدفع الإلكتروني: الجزائر نموذجا، المركز الجامعي عبد الحفيظ بو الصوف. ميلة، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي ضرورة الانتقال وتحديات الحماية.
- المطيري، سعد فهد ادبيس. (2023). مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية، كلية الحقوق، جامعة عين شمس.

- معهد الدراسات المصرفية. (2023). خدمات بطاقات الدفع الإلكتروني والدفع المسبق، والدفع عن طريق الهاتف النقال، إضاءات، السلسلة 15، العدد 5، دولة الكويت.
- مقلاتي، مونة؛ مشري، راضية. (2021). الجريمة الإلكترونية دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، مج6، ع1.
- موسى، محمود علي؛ أبو عكر، محمد نايف. (2023). الخوف من الجريمة الإلكترونية المستهدفة للأفراد وعلاقته بالقلق الاجتماعي لدى عينة من الشباب، المجلة العربية للدراسات الأمنية، جامعة قناة السويس، مصر.
- هيئة الحكومة الرقمية (2023). الإحتيال الرقمي . دراسة بحثية
- وهدان، أحمد (2024). المحافظ الإلكترونية وأثرها في تغيير مستقبل قطاع المدفوعات. وكالة الأنباء السعودية . موقع ومضة حاضنة لريادة الأعمال .
- وهيبة، عبد الرحيم. (2010). تقييم وسائل الدفع الإلكترونية ومستقبل وسائل الدفع التقليدية في ظل وجودها، المركز الجامعي لتمرست، مجلة الاقتصاد الجديد، ع2.
- ثانياً: المراجع باللغة الإنجليزية :**

1. Alyabes, Alhanoof and Alsalloum, Othman (2018) . **Factors Affecting Consumers' Perception of Electronic Payment in Saudi Arabia** . King Saud University.
2. Ben Krishna and Satish Krishnan and M. P. Sebastian (2022) . **National Cybersecurity Commitment and Digital Payment Usage** . journal Information Systems Frontiers _.
3. Gupta ,Pranay and T. Mandy (2019). **FinTech: The New DNA of Financial Services**_. Walter de Gruyter Inc .
4. Alotaibi, Fawaz and Stengel, Istvan and Papadaki, Maria (2016). **Awareness of Cybercrimes among Internet Users in Saudi Arabia** . Transactions (ICITST) held in Barcelona, Spain

ثالثاً: مواقع الجهات الحكومية في المملكة العربية السعودية :

١. [المنصة الوطنية للخدمات الحكومية\(my.gov.sa\)](http://my.gov.sa)
٢. [هيئة الحكومة الرقمية\(dga.gov.sa\)](http://dga.gov.sa)
٣. [وزارة التجارة\(mc.gov.sa\)](http://mc.gov.sa)
٤. [البنك المركزي السعودي\(sama.gov.sa\)](http://sama.gov.sa)
٥. [هيئة السوق المالية\(cma.org.sa\) | Capital Market Authority](http://cma.org.sa)

الملاحق

ملحق رقم (1)



استبيان موجه للمستهلكين

السادة

السلام عليكم ورحمة الله وبركاته

تجري الباحثة بحثاً علمياً بعنوان:

مخاطر خدمات الدفع الإلكتروني وعلاقتها بحدوث الجرائم الإلكترونية "دراسة تطبيقية

على قطاع خدمات المدفوعات بالمملكة العربية السعودية"

لذا آمل من سعادتك التكرم بالإجابة على الأسئلة المرفقة، مع العلم أن كافة المعلومات

التي سيتم الحصول عليها ستستخدم لأغراض البحث العلمي فقط.

تقبلوا فائق الاحترام والتقدير

الباحثة

ندى منصور بن داود

233001438

القسم الأول: معلومات شخصية

الرجاء وضع علامة (X) بجانب الخيار الصحيح:

أولاً- البيانات الشخصية:

1. المؤهل العلمي:

- بكالوريوس
- ماجستير
- دكتوراه
- أخرى تذكر.....

2. الجنس:

- ذكر
- أنثى

القسم الثاني: محاور الاستبيان

الرجاء وضع علامة (X) في الخانة المناسبة

المحور الأول: خدمات الدفع الإلكتروني التي يستخدمها العملاء في المملكة العربية السعودية من وجهة نظر المستهلكين:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	أستخدم خدمات الدفع الإلكتروني بشكل يومي ومتكرر .					
2.	أستخدم خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات.					
3.	أستخدم خدمات الدفع الإلكتروني لإمكانية الشراء عبر الإنترنت من المواقع الإلكترونية					
4.	أستخدم خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول أو البطاقات الائتمانية					
5.	أستخدم خدمات الدفع الإلكتروني لإمكانية تحويل الأموال عبر المحافظ وإجراء المعاملات المالية وشحن الرصيد .					

المحور الثاني: المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر المستهلكين:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	تحمل خدمات الدفع الإلكتروني مخاطر عالية تتعلق بالاختراقات الأمنية					
2.	استخدام خدمات الدفع الإلكتروني يمكن أن يعرضني للاحتيال المالي					
3.	هناك احتمالية كبيرة لفقدان بياناتي الشخصية عند استخدام خدمات الدفع الإلكتروني.					
4.	هناك خطرًا من إساءة استخدام معلوماتي من قبل موظفي الشركات المقدمة لخدمات الدفع الإلكتروني.					
5.	هناك نقصًا في الدعم والمساعدة الفورية في حالة تعرضي لمشكلات أمنية أثناء استخدام خدمات الدفع الإلكتروني.					

المحور الثالث: العوامل التي تسهم في تقليل مخاطر الدفع الإلكتروني من وجهة نظر المستهلكين:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	ربط وسائل الدفع الإلكتروني بوسائل أمان تساعد في تحديد هوية العملاء .					
2.	استخدام أساليب متقدمة للمصادقة .					
3.	تجريم جميع الأفعال التي فيها مساس بالأنظمة الإلكترونية ومستخدميها					
4.	تشفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها .					
5.	استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية					

المحور الرابع: تأثير مخاطر خدمات الدفع الإلكتروني على مستوى الأمان والثقة لدى مستخدمي هذه الأنظمة.

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	تقدم البنوك والمؤسسات المالية في المملكة مستوى عالٍ من الحماية لمستخدمي خدمات الدفع الإلكتروني					
2.	تعرضت لجرائم إلكترونية مرتبطة بخدمات الدفع الإلكتروني.					
3.	من الممكن اختراق حساباتي عند استخدام خدمات الدفع الإلكتروني.					
4.	المخاطر المرتبطة بخدمات الدفع الإلكتروني تؤثر على قراري باستخدامها في المعاملات المالية الكبيرة.					
5.	أفضل استخدام النقد أو وسائل الدفع التقليدية بسبب المخاوف الأمنية من الدفع الإلكتروني					
6.	أنا على استعداد لدفع رسوم إضافية مع السداد عند الاستلام عوضاً عن الدفع الإلكتروني بسبب قلقي من مخاطر الدفع الإلكتروني.					

					7. خدمات الدعم الفني المتاحة تساعدني في التعامل مع المشكلات الأمنية عند استخدام خدمات الدفع الإلكتروني
--	--	--	--	--	--

المحور الخامس: وعي المستهلكين بمخاطر وسائل الدفع الإلكتروني لمنع حدوث الجرائم:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	تحقق دائماً من صحة المواقع والتطبيقات التي تستخدمها للدفع الإلكتروني قبل إدخال بياناتك المالية.					
2.	تقديم معلوماتك المالية عبر الإنترنت يمكن أن يتعرض لخطر الاختراق أو الاستخدام غير المصرح به.					
3.	أفضل تلقي تنبيهات فورية عندما يتم استخدام حسابي أو بطاقتي لعمليات دفع غير معتادة أو غير مصرح بها.					
4.	أفضل استخدام خدمات الدفع الإلكتروني التي توفر تقنيات تحقق إضافية مثل الرموز السرية أو التحقق الثنائي لتعزيز الأمان.					
5.	أقوم بتحديث برامج الحماية المضادة للفيروسات بانتظام لحماية جهازي من					

					البرمجيات الخبيثة التي قد تهدد معلوماتي المالية عند استخدام الدفع الإلكتروني.
					6. أشارك في التدريبات أو الدورات التي تعزز من وعي بأمان الدفع الإلكتروني وكيفية حماية معلوماتي المالية عبر الإنترنت.

المحور السادس: التدابير التي يمكن أن يتبناها المستهلك للحد من هذه المخاطر والجرائم:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	استخدام كلمات سر قوية					
2.	التصريح الفوري حال ضياع البطاقة الإلكترونية أو فقدانها					
3.	التحقق الدوري من الحسابات المالية لاكتشاف أي نشاط غير طبيعي او مشبوه					
4.	اعتماد تطبيقات ومواقع الدفع الآمنة					
5.	متابعة أحدث المستجدات والممارسات الأمنية في مجال الدفع الإلكتروني					
6.	تحديث نظام التشغيل، المتصفح، وبرامج الحماية من الفيروسات بشكل دوري					

ملحق رقم (2)



استبيان موجه للعاملين

السادة

السلام عليكم ورحمة الله وبركاته

تجري الباحثة بحثاً علمياً بعنوان:

مخاطر خدمات الدفع الالكتروني وعلاقتها بحدوث الجرائم الالكترونية دراسة تطبيقية على

قطاع خدمات المدفوعات بالمملكة العربية السعودية

لذا آمل من سعادتك التكرم بالإجابة على الأسئلة المرفقة، مع العلم أن كافة المعلومات

التي سيتم الحصول عليها ستستخدم لأغراض البحث العلمي فقط.

تقبلوا فائق الاحترام والتقدير

الباحثة

ندى منصور بن داود

233001438

القسم الأول: معلومات شخصية

الرجاء وضع علامة (X) بجانب الخيار الصحيح:

أولاً- البيانات الشخصية:

1. المؤهل العلمي:

- بكالوريوس
- ماجستير
- دكتوراه
- أخرى تذكر.....

2. المنصب الوظيفي:

- موظف
- رئيس قسم.
- مشرف.
- أخرى تذكر.....

3. سنوات الخبرة:

- أقل من سنتين.
- من ثلاث سنوات إلى خمس سنوات.
- فوق الست سنوات.

القسم الثاني: محاور الاستبيان

الرجاء وضع علامة (X) في الخانة المناسبة

المحور الأول: خدمات الدفع الإلكتروني التي يستخدمها العملاء في المملكة العربية السعودية من وجهة نظر العاملين:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	يستخدم العملاء خدمات الدفع الإلكتروني بشكل يومي ومتكرر .					
2.	يستخدم العملاء خدمات الدفع الإلكتروني من أجل تسديد الفواتير والاشتراكات.					
3.	يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية الشراء عبر الإنترنت من المواقع الإلكترونية					
4.	يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية الدفع في المتاجر الفعلية عن طريق الهاتف المحمول او البطاقات الائتمانية					
5.	يستخدم العملاء خدمات الدفع الإلكتروني لإمكانية تحويل الأموال عبر المحافظ وإجراء المعاملات المالية و شحن الرصيد.					

المحور الثاني: المخاطر المرتبطة بخدمات الدفع الإلكتروني من وجهة نظر العاملين:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	خدمات الدفع الإلكتروني تحمل مخاطر عالية تتعلق بالاختراقات الأمنية.					
2.	خدمات الدفع الإلكتروني تساهم في زيادة مخاطر غسل الأموال وتمويل الإرهاب.					
3.	استخدام خدمات الدفع الإلكتروني تعرض العميل للاحتيال المالي.					
4.	هناك احتمالية كبيرة لفقدان بيانات العميل الشخصية عند استخدام خدمات الدفع الإلكتروني.					
5.	هناك خطرًا من إساءة استخدام معلومات العميل من قبل بعض موظفي الشركات المقدمة لخدمات الدفع الإلكتروني					
6.	هناك نقصًا في الدعم والمساعدة الفورية في حالة تعرض العميل لمشكلات أمنية أثناء استخدام خدمات الدفع الإلكتروني.					

المحور الثالث: العوامل التي تساهم في تقليل مخاطر خدمات الدفع الإلكتروني من

وجهة نظر العاملين.

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	ربط وسائل الدفع الإلكتروني بوسائل أمان تساعد في تحديد هوية العملاء .					
2.	استخدام أساليب متقدمة للمصادقة .					
3.	تجريم جميع الأفعال التي فيها مساس بالأنظمة الإلكترونية ومستخدميها					
4.	تشفير بيانات المستهلكين حتى لا يسهل الوصول إليها واختراقها .					
5.	استخدام البرامج المضادة لفيروسات وتكنولوجيا الجدران النارية					
6.	التحديث المستمر للبرامج والنظم					
7.	الاحتفاظ بنسخ احتياطية للبيانات الموجودة					
8.	استخدام جهاز قارئ للبطاقة يقوم بقراءة معلومات وسائل الدفع الإلكتروني					
9.	الالتزام بفحص صحة عمليات الدفع الإلكتروني من خلال الاستعانة بالتقنيات الحديثة					

					10. توعية العملاء بأهمية اتباع ممارسات الأمان عند استخدام خدمات الدفع الإلكتروني وعدم مشاركة معلوماتهم الشخصية مع الآخرين
--	--	--	--	--	---

المحور الرابع: مخاطر الدفع الإلكتروني وعلاقته بالجرائم الإلكترونية من وجهة نظر العاملين:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	عدم القيام بفحص كافٍ للعملاء قد يؤدي إلى استخدام الحسابات بطرق غير مشروعة أو لأنشطة غير قانونية.					
2.	عدم إجراء مراجعات دورية ومنتظمة للحسابات والنظم قد يمكن للمحتالين من استغلال الثغرات والضعف في النظام.					
3.	عدم توفير التدريب المناسب للموظفين حول كيفية التعامل مع الجرائم المالية والتهديدات الأمنية يمكن أن يترك الشركة عرضة للمخاطر					

					4. عدم وجود إجراءات واضحة للتبليغ عن الجرائم المالية قد يمكن المجرمين من العمل دون أن يتم اكتشافهم بسرعة.
					5. الاعتماد على تقنيات قديمة أو غير محدثة قد يجعل الأنظمة عرضة للاختراقات والهجمات الإلكترونية.
					10. عدم وجود سياسات صارمة لإدارة المخاطر المالية والأمنية قد يجعل من الصعب اكتشاف ومواجهة الاحتيال والجرائم المالية.
					11. عدم فرض رقابة صارمة على من يتمتعون بصلاحيات الوصول إلى البيانات والأنظمة يمكن أن يؤدي إلى الوصول غير المصرح به واستخدامه بشكل غير قانوني
					12. عدم السرعة في التعامل مع الشكاوي والمشكلات الأمنية التي تواجه العميل أثناء استخدام خدمات الدفع الإلكتروني.

المحور الخامس: التدابير التي يمكن أن تتبعها المنظمة للحد من هذه المخاطر والجرائم:

رقم الفقرة	الفقرات	أوافق بشدة	أوافق	محايد	غير موافق	غير موافق بشدة
1.	التحقق من مخاطر العميل قبل الدخول معه في علاقة عمل والربط مع جهات حكومية موثوقة للتحقق من هوية العميل.					
2.	استخدام بروتوكول آمن بين المستخدم والخادم المالي، يستخدم طبقة تشفير لحماية البيانات المرسلة والمستقبلية .					
3.	استخدام توثيق متعدد العوامل لتأكيد هوية المستخدم في عملية الدفع الإلكتروني.					
4.	الاستثمار في تحديث التقنيات وتطوير البنية التحتية .					
5.	الاستفادة من خبرات الخبراء في أمن المعلومات يمكن أن تساهم في تعزيز أمان خدمات الدفع الإلكتروني					
6.	التحليلات البيانية والذكاء الاصطناعي يساهم في التنبؤ بالتهديدات الأمنية					
7.	وجود تعاون بين مختلف الأطراف في قطاع خدمات الدفع الإلكتروني يساهم في تعزيز الأمان والحد من الجرائم الإلكترونية					

					8. تنظيم دورات تدريبية وتوعية العاملين بانتظام حول كيفية اكتشاف ومنع الجرائم المالية، بما في ذلك التعرف على أساليب الاحتيال الشائعة والإجراءات الأمنية اللازمة لحماية المعلومات المالية
					9. فرض قيود جغرافية على المعاملات المالية، بحيث يتم قبول المعاملات فقط ضمن مناطق محددة ومعروفة مسبقاً، مما يساعد في تقليل فرص الاحتيال والجرائم المالية