جـــامـعـة الـــشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

The Impact of Perceived Information Security on Mobile Commerce Customer Satisfaction:

A Field Study in Jordanian Private Universities in Amman

أثر أمن المعلومات المدرك على رضا زبون التجارة الالكترونية المحمولة:

دراسة ميدانية على الجامعات الخاصة الأردنية في عمان

Prepared by

Aidmar Biltawi

Supervised by

Prof. Ahmad Al-Sukkar

Thesis Submitted in Partial Fulfilment of the Requirements for Master Degree in E-Business.

Management Department

Business Faculty

Middle East University

January 2019

Authorization

I am **Aidmar Hasan Biltawi** authorize Middle East University for Graduate Studies, to provide hard or electronic copies of my thesis to libraries, organizations, or institutions concerns in academic research upon request.

Name: Aidmar Hasan Biltawi

Date: 29 / 01 / 2019.

Signature: 

Committee Discussion and Decision

This thesis of the student Aidmar Hasan Biltawi, which studied "**The Impact of Perceived Information Security on Mobile Commerce Customer Satisfaction: A Field Study in Jordanian Private Universities in Amman**", has been defined, accepted and approved on 29th of January 2019, by the following committee members:

Committee Members:

No	Academic Rank	Discussion Committee	Title	Signature
1	Associate Prof.	Ahmad Saleh Al-Sukkar	Supervisor and Head of the Committee	
2	Associate Prof.	Fayez Ahmad Al-Badri	Internal Examiner	
3	Associate Prof.	Fadi Taher Qutaishat	External Examiner	

Acknowledgement

I am profoundly grateful to God, the Wise, the Truth, the Real, for always being there when I need his guidance and sympathy.

I would also like to extend many thanks to my supervisor Prof. Ahmad Al-Sukkar, for keeping me on the right track and helping me complete my thesis.

Finally, Heartfelt thanks to the discussion committee for taking their time and effort, reviewing my thesis.

Aidmar Hasan Biltawi

Dedication

To my Father, without you I would probably never amount to much, you are the bedrock of my foundation. To my Mother in heaven, I hope you're proud of me and I miss you. To my Wife, thank you for standing by me, without you, I would go astray. To my Brothers, I know I can always count on you. To my Great Aunt whose support and grace, brightened my future. Finally, to myself, I made it.

Aidmar Hasan Biltawi

Table of Contents

LIST OF TABLES

List of Figures

List of Appendix

The Impact of Perceived Information Security on Mobile Commerce Customer Satisfaction
A Field Study on Jordanian Private Universities in Amman

Prepared by:

Aidmar Hasan Biltawi

Supervised by:

Prof. Ahmad Al-Sukkar

Abstract

The purpose of this study was to examine the impact of perceived information security on mobile commerce customer satisfaction in Jordanian private universities in Amman. In order to achieve the objectives of this study, descriptive analytical methods were used to classify and analyze the data collected from a sample respondent size of 282. The sample respondents were university students and a questionnaire was used and handed out under supervision to collect the data, which was thereafter tested for normality, validity and reliability. The (SPSS) descriptive analysis was conducted and the correlation between the variables were checked. The findings of this study found that there is an impact of perceived information security at the significant level ($a \leq 0.05$) on mobile customer satisfaction, the results also indicate that the element (Confidentiality) has a statistically significant effect on customer satisfaction, and the rest of the elements (Authentication, Non-Repudiation, Integrity) have a positive effect that is apparent but no statistically significant. The practical implications of this study require further development of mobile commerce information security architectures that is developed as technology develops, while also requiring security measures to advance towards a safe and secure practices. As per recommendations, this study recommends future researchers to expand on mobile commerce customers' perception of security and its impact on satisfaction, by adding more variables from other mobile commerce security architectures. This study is considered as the only study to tackle the issue of perceived information security on mobile commerce customer satisfaction, conducted in private Jordanian universities.

Keywords: Perceived Information Security, Mobile Commerce, Customer Satisfaction, Jordanian Private Universities, Authentication, Non-Repudiation, Integrity, Confidentiality.

أثر أمن المعلومات المدرك على رضا زبون التجارة الالكترونية المحمولة: دراسة ميدانية على الجامعات الخاصة الأردنية في عمان

إعداد:

ايدمر حسن بلتاوي

اشراف:

الدكتور احمد السكر

الملخص

تهدف هذه الدراسة الى البحث في أثر أمن المعلومات المدرك على رضا زبون التجارة الالكترونية المحمولة في طلاب الجامعات الاردنية الخاصة في عمان. ومن أجل تحقيق أهداف هذه الدراسة، تم استخدام منهجية التحليل الوصفي الاحصائي في تحليل البيانات التي تم جمعها من عينة الطلاب وعددها 282 استبانة. وتم التأكد من التوزيع الطبيعي وصدق وثبات اداة الدراسة، وتم اجراء تحليل وصفي وتحقق من ارتباط المتغيرات وأختبار التأثير بواسطة الانحدار المتعدد. أظهرت النتائج بأن هنالك تأثير لأمن المعلومات المدرك على مستوى عالي على رضا الزبون. كما تظهر النتائج بأن عنصر(السرية) له تأثير مهم من ناحية أحصائية على رضى الزبون. أما بقية العناصر (مصادقة الهوية، عدم إنكار التنصل، سلامة البيانات) فلها تأثير إيجابي واضح، ولكن ليس بدلالة إحصائية. أما بالنسبة للتطبيقات العملية لهذه الدراسة. إن متطلبات أمن المعلومات ضرورية لرضا الزبون في التجارة الإلكترونية المحمولة وبالتالي فهم مدركات واهتمامات ومخاوف الزبون مهمين لتطوير بنية أمنة للتجارة الالكترونية المحمولة. ويجب مواكبة التطورات التكنولوجييا واللوازم الامنية في بناء تدابير أمنية تحمي الزبون من خلال استغلال أفضل الممارسات. وتوصي هذه الدراسة بأن يتم توسيع البحث في مجال أمن المعلومات المدركة لدى زبون التجارة الالكترونية المحمولة من خلال اختبار المزيد من المتغيرات وفهم المخاوف التي تأثر على رضا الزبون.

الكلمات المفتاحية: أمن المعلومات المدرك، التجارة الالكترونية المحمولة، رضا الزبون، طلاب الجامعات الخاصة، مصادقة الهوية، عدم إنكار التنصل، سلامة البيانات، السرية.

General Framework

1.1 Introduction

Almost everyone nowadays has a mobile smart device. They are used for multiple things, such as; searching for a place to eat or te recipie to make the food, checking the address for a location, sharing our opinions online on certain subjects, communicating with each other, and even finding love. These smart devices are very important not only for uses in commerce, but many other things. There is an insurmountable amount of transactions that occurring every day through mobile devices, with that comes risk, and with risk comes the need to secure these transactions, for it is essential not just for mobile commerce to actually function, but also the effect it has on its customers.

It is quiet strange to find a person without a mobile device these days. In recent years, people have developed a dependency relationship with their mobile devices, which lead to the development of an actual anxiety disorder, related to the fear of operating through the day, without a mobile device, or beyond mobile phone contact. Such anxiety disorder is named Nomophobia (Elmore, 2014). Due to the high dependence on mobile devices in this generation to keep us connected, updated and online, since these devices enable its users to access and view useful information quickly and when needed. Unsurprisingly, these devices are also collecting a host of data on its users and their habit and behavior, all of the time, to be used by businesses or governments (Nield, 2018).

Modern smartphones are packed with many powerful sensors that enable the device to collect data about its users. Mobile smart devices contain more sensors than most anyone realizes, Their sensors include, audio, video, touch,

acceleration, light, proximity, GPS sensors (Weiss, 2013). Because of the large amount of information and the benefits that mobile devices provide, most businesses develop their own mobile application, causing an (app) ecosystem to become one of the largest industries in the world, encapsulating millions of app developers (Boxall, 2016), and billions of mobile smart device owners, who use mobile apps in their day to day activities. Recent statistics provide a forecast of 197 billion mobile app downloads in 2017 (The Statistics Portal, 2018), with most popular app categories being those of games, social networking, entertainment, news, as well as health fitness and lifestyle (ENISA, 2017).

With mobile devices on Internet, came a variety of security concerns for manufacturers, developers and customers. These devices are connected to email addresses; cloud-based storage networks, and it is raising concerns for customers that need increased data security and privacy protection to include personally identifiable information. On the other hand, the increase in demand for mobile security to protect data and privacy have forced manufacturers and software developers to explore new ways to strengthen mobile security (Shea, 2015). According Xu & Yang (2012) “It is vital to understand the point of view of mobile commerce customers to ensure the successful implementation of mobile commerce applications. Since it would improve the business process, and address privacy and security concerns”.

Apps on mobile devices are either a native application that comes with the operating system or developed as a web app found on a mobile app store (Charland & LeRoux, 2011). Mobile-apps cover most of the customers activities on smartphones, that inevitably gave rise for the saying; there is an app for that (Douglas, Wojcik, & Thompson, 2012) According to (Mylonas, Kastania, & Gritzalis, 2013) there

has been a pervasive lack of awareness among mobile device users concerning security and privacy risks associated with downloading apps, since most people who were surveyed concerning app markets assumed that controlled app marketplaces such as (e.g., Google Play) are secure. In current days, the most popular Mobile operating systems have been Android and Apple iOS in consumer space. Amongst them, Android operating system has majority of the market share, 2.6 Million apps in Google Play and 2.1 Million Apps in Apple's App Store in 2018 (The Statistics Portal, 2018).

Mobile Commerce depends on web apps to conduct business; most customers are unaware to the security issues that could compromise them when operating on a wireless network, and how they are prone to passive attacks. Customers have major concerns about the information they share from unauthorized party gaining access, while, identification and message integrity are also involved in mobile security and is a major concern (Wushishi & Ogundiya, 2014). Privacy and security are very important issues in mobile commerce implementation, and the users of mobile commerce, expect certain protocols to be put in place to protect their privacy and security. To address the customer concerns when using mobile commerce services, certain expectations must be fulfilled in order to attain mobile commerce customer satisfaction (Xu & Yang, 2012). The data recovered from the 2018 Strategic Security survey, suggests that "organizations are going to increase spending on security in their products and technologies. A 40% increase is expected to be spent on information security in 2018 than they did in 2017" (Doherty, 2018).

Therefore, the purpose of this thesis was to measure the impact of perceived information security and its factors on mobile commerce customers (university students) satisfaction.

1.2 Study Problem

Information security is developing with technological advancement, and is essential to the functioning of any industry that uses information systems such as mobile commerce. Customers (University students) of mobile commerce expect security in mobile commerce transactions, which is essential to a satisfactory experience. While mobile commerce growth exploded with mobile device use, new threats arise to mobile commerce security which would affect customer satisfaction.

As such aspects in information security models and architectures in mobile commerce, must be studied to identify which aspects are perceived and require attention to better satisfy its users and to give developers a better understanding of customer needs and concerns in mobile commerce information security.

As discussed earlier the main problem of this thesis is to investigate the impact of perceived information security on mobile commerce customer satisfaction through study objectives and questions.

1.3 Study Objectives

The main objective of this thesis, is to examine the impact of perceived information security on mobile commerce customer satisfaction, and in order to achieve this. The following objectives were set:

- To provide a theoretical framework based on the variables of the current study of Perceived Information Security, Authentication, Non-Repudiation, Integrity, Confidentiality – Mobile Commerce, Customer Satisfaction.
- To determine the level of mobile commerce customer satisfaction for the private university students.

- To identify the factors that affect mobile commerce customer satisfaction in perceived information security and the impact of perceived information security on mobile commerce customer satisfaction.
- To examine the impact perception of the variables in information security.
- To produce a number of recommendations for further research in the subject.

1.4 Study Significance

This study may be considered one of the few local study that conduct the impact of perceived information security on customer satisfaction on private university students in the Jordanian mobile commerce sector.

The result of this study would be important to mobile commerce developers and organizations, while also alerting customers to the security dimensions that they are perhaps unaware of when using mobile commerce services.

Therefore, the importance of this study was derived from the importance of the variables that are dealing with and following scientific and practical considerations: To highlight the nature and importance of information security in mobile commerce for the benefit of the developers, customers and users of mobile commerce. While also providing a comprehensive survey of the study variables concepts and dimensions that can be relied upon to measure the study variables, so that it can benefit researchers and practitioners as a starting point for their future research, and to provide a systematic basis in the field of measuring perceived information security impact on mobile commerce customer satisfaction that may help to rely on measures that have a high degree of reliability and validity. The highlighting the nature and importance of information security in mobile commerce for the benefit of the customers and users of mobile commerce.

The subject of the information security of mobile commerce applications is very sophisticated and renewed in accordance with the changes and developments in technology, so it is found that the studies on this subject continue as long as technological development continues, which called for the current study.

1.5 Study Questions and Hypotheses

Based on the study problem, the study will investigate the following questions:

1. Does Percieved Information Security have an impact on Mobile Commerce Customer Satisfaction in Jordanian Private Universities?

Based on the percieved information security measures implemented in mobile commerce the main question is divided in the following sub-questions:

1.1. Does Authentication have an impact on Mobile Commerce Customer Satisfaction in Jordanian Private University Students?

1.2. Does Non-Repudiation have an impact on Mobile Commerce Customer Satisfaction in Jordanian Private University Students?

1.3. Does Integrity have an impact on Mobile Commerce Customer Satisfaction in Jordanian Private University Students?

1.4. Does Confidentiality have an impact on Mobile Commerce Customer Satisfaction in Jordanian Private University Students?

Based on problem statement the following hypotheses were derived:

H1: There is a statistically positive impact of Percieved Information Security on Mobile Commerce Customer Satisfaction among students of Jordanian private universities at level ($\alpha \leq 0.05$).

Based on the measures of Percieved Information Security, the main hypothesis was divided into the following sub-hypotheses:

H1.1: There is a statistically positive impact of Authentication on Mobile Commerce Customer Satisfaction in Jordanian Private University Students, at level ($\alpha \leq 0.05$).

H1.2: There is a statistically positive impact of Non-Repudiation on Mobile Commerce Customer Satisfaction in Jordanian Private University Students, at level ($\alpha \leq 0.05$).

H1.3: There is a statistically positive impact of Integrity on Mobile Commerce Customer Satisfaction in Jordanian Private University Students, at level ($\alpha \leq 0.05$).

H1.4: There is a statistically positive impact of Confidentiality on Mobile Commerce Customer Satisfaction in Jordanian Private University Students, at level ($\alpha \leq 0.05$).

1.6 Study Model

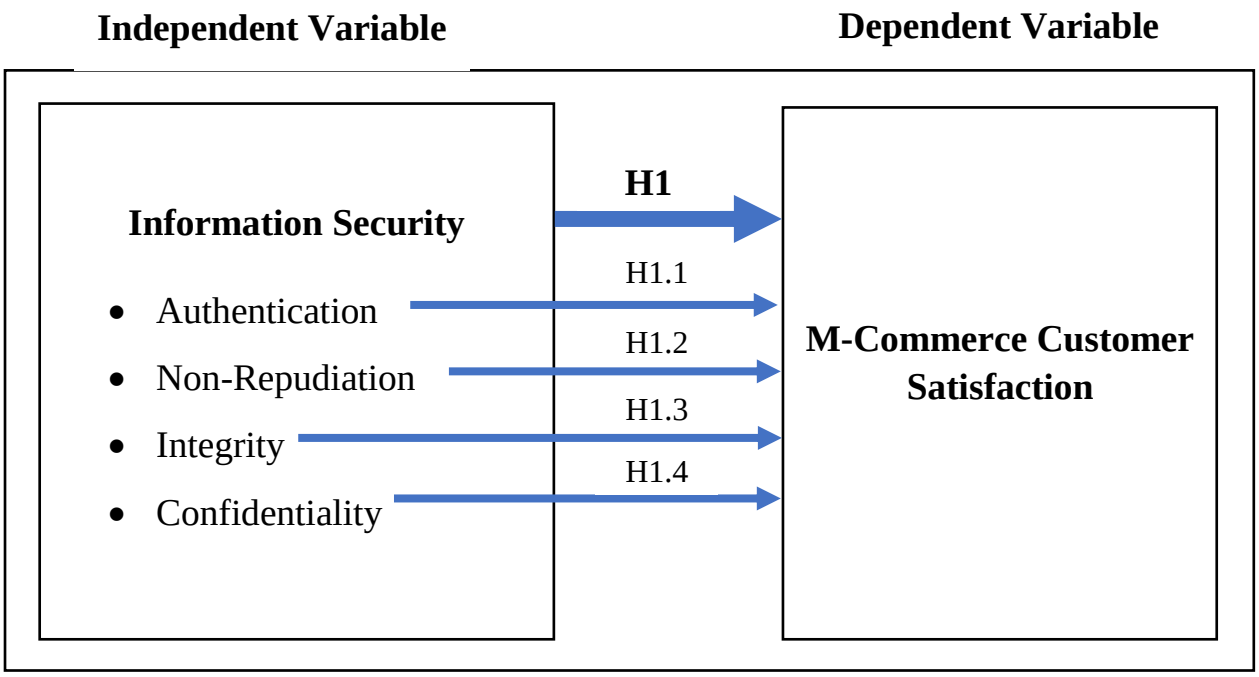

Figure 0-1: Study Model

Source: prepared by the researcher based on previous studies:

Independent Variable: (Wei, Liu, & Koong, 2006) (Wei & Ozok, 2009) (Beyer, 2014) (Ojha, 2015) ***Dependent Variable:*** (Jiradilok, Malisuwan, Madan, & Sivaraks, 2014)

1.7 Study Limitations

There are number of limitations for this thesis:

- **Human limitation:** This study was carried on University students.
- **Place limitation:** This study was conducted with Jordanian private universities in Amman.
- **Time limitation**: the academic year 2018-2019.
- **Scientific limitation:** This study focused on the impact of percieved information security on mobile commerce customer satisfaction and adapted prior studies recommendations.

1.8 Study Delimitations

This study was implemented on private Jordanian university students in Amman, which was homogenous and representative of study population.

- Study results was restricted only on Jordanian private universities students - Amman.
- The amount of collected data depended on private university student's response to the questionnaires.
- The university student's response reflected the psychological impression of information security in mobile commerce at that point of time.

1.9 Study Conceptual Definitions

- ***Mobile Commerce (M-Commerce):*** Defined as "any transaction that involves buying and/or selling any products or services with a monetary value through a mobile device using a wireless network" (Jimenez, San-Martin, & Azuela, 2016)
- ***Cybersecurity*****:** Defined as *"*the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation." (NATO, 2016).
- ***Information Security:*** Defined as "a discipline, the main aim of which is to keep the knowledge, data and its meaning free from undesirable events, such as theft, espionage, damage, threat and other danger. Information security includes all actions, taken in advance, to prevent undesirable events happening to the knowledge, data and its meaning so that the knowledge, data and its meaning could be relied on (Cherdantseva & Hilton, 2013).
- ***Information Assurance***: Defined as " a discipline, the main aim of which is to give confidence or certainty in information; to give belief that one can rely on data, knowledge, facts, and its meaning (Cherdantseva & Hilton, 2013)."
- ***Authentication:*** Defined as *"*the process of verifying the identity or other attributes of an entity (user, process or device). also, the process of verifying the source and integrity of data (NATO, 2016).
- ***Non-Repudiation***: Define as "assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information (Cherdantseva & Hilton, 2013).

- ***Integrity:*** Defined as “ensures that information has not been modified or altered during a transmission (Wei & Ozok, 2009).”
- ***Confidentiality***: Defined as “the property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information (Cherdantseva & Hilton, 2013).”
- ***Customer Satisfaction*** Defined as “ when products and services meet the expectation of the consumers (Jiradilok, Malisuwan, Madan, & Sivaraks, 2014).

Chapter 1 Theoretical Framework and Previous Studies

2.1 Theoretical Framework.

2.1.1 Mobile Commerce

Mobile commerce is simply the buying and selling through a wireless network using a mobile device by issuing transactions of information, goods or services (Said & Noordin, 2011), some of the services that mobile commerce provides are as follows: mobile financial services, mobile advertisement, mobile entertainment, mobile shopping (Giri & Singh, 2014). The ubiquitous nature of mobile commerce is what drives its growth, since people can use their mobile devices anywhere, anytime (Shamsi & Afzal, 2017). Online satisfaction is divided into 3 main factors and 9 sub factors: 1. Information quality: Entertainment and Informativeness 2. System quality: Access and Interactivity 3. Service quality: Reliability, responsiveness, assurance, tangibility and empathy (Jiradilok, Malisuwan, Madan, & Sivaraks, 2014).

2.1.2 Perceived Information Security

Information security is “a matter of understanding and managing risk, and not eliminating threats. When every functional computing device is also a networked computing device, there is no such thing as an absolutely secure information system” (Budzak, 2016). The “increase in security threats to IT appliances has made the problem of information security a great concern for IT users” as (Hung, Rau, Salvendy, & Shang, 2008) states. Information security is concerned in protecting all types of information regardless of type (e.g. visual, text, electronic or even paper), and includes all actions that protect information in processing, transmission and storage, protecting information from undesirable events such as theft, eavesdropping or tamper, and in summary to eliminate threats (Cherdantseva & Hilton, 2013). There are many security

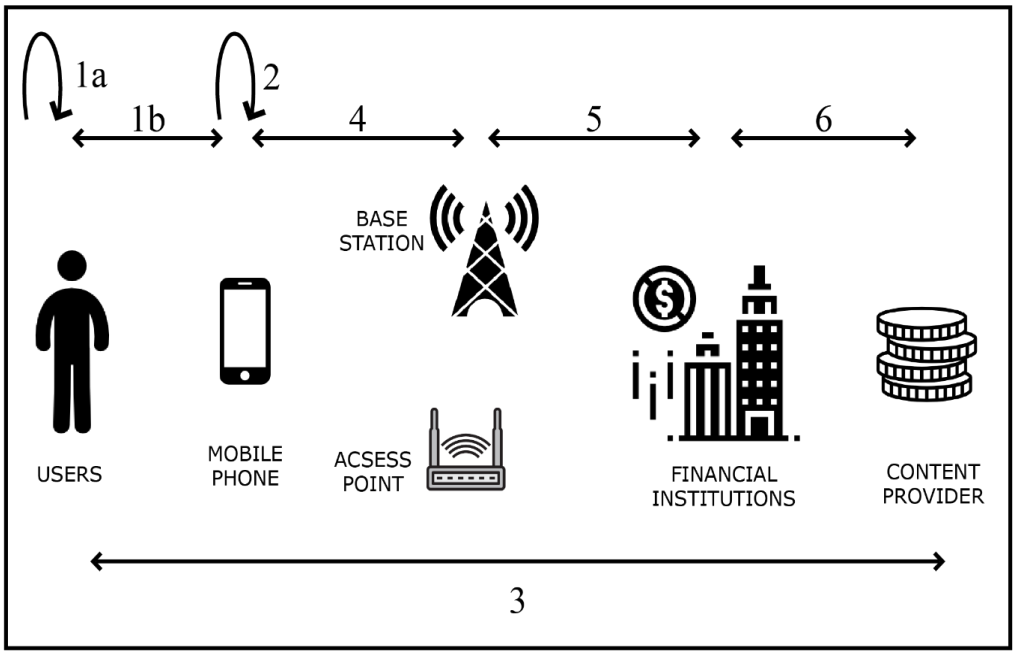

Figure 1-1: Levels of Vulnerability in Mobile Commerce (Marufu, 2013)

models developed in information security for all s`orts of information technology and main focus of this study is the security model created for the mobile commerce context as we continue to discover in the literature the different levels of vulnerability and the threats mobile commerce faces and has to handle.

There are six levels of vulnerability in Mobile Commerce: as shown in Figure (2-1) (Marufu, 2013).

- human aspect (1a, 1b),
- mobile device security (2),
- Mobile Commerce access channel, (3)
- access network infrastructure (4),
- serve side and back end systems security (5.6)

Table 1-1: Mobile Device Threats (Marufu, 2013)

Dimensions	T.No	Threat
Network	T1	Spoofing
Connectivity	T2	Scanning
	T3	Denial of Service, Network Congestion
	T4	Spam, Advertisment
	T5	Eavesdropping
	T6	Jamming
Device	T7	Loss, Theft, Disposal or Damage
	T8	Cloning SIM Card
	T9	Technical Failure of Device
	T10	Unauthorized Device (Physical) Access
	T11	Unauthorized Access
	T12	Offline Tampering
Operating System	T13	Crashing
	T14	Misuse of Phone Identifiers
	T15	Electronic Tracking Survilliance Exposure of Physical Location
	T16	Resource Abuse
Applications	T17	Sensitive Information Disclosure (SID), Spyware
	T18	Corrupting or Modifying Private Control
	T19	Disabling Applications or the Device
	T20	Client-Side Injection Malware
	T21	Direct Billing
	T22	Phishing

There are many threats to mobile devices as shown in Table (2-1), because of the different levels of mobile commerce vulnerability and threats, there is a need for a multi-layered architecture. The onion ring architecture as shown in Figure (2-2) offers conceptual simplicity and excellent security, by matching and sorting access rights to increasing levels of responsibility. (Wei, Liu, & Koong, 2006).

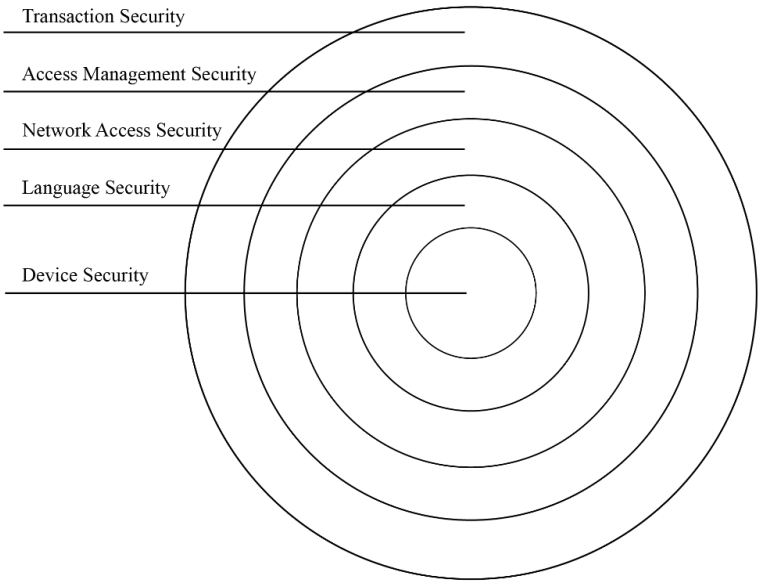

Figure 1-2: An 'onion ring' framework for M-Commerce security (Wei, Liu, & Koong, An onion ring framework for developing and assessing mobile commerce security, 2006)

Each layer in the framework organizes and handles different levels of security as shown in Table (2-3) as shown below, which offers a brief of the different framework layers.

Table 1-2: A brief over the layers in the framework (Wei, Liu, & Koong, An onion ring framework for developing and assessing mobile commerce security, 2006)

Layer One	**Mobile Commerce Device Security Layer**
	The root layer to enable mobile commerce security that is inherent in all the mobile communication devices, because they are the front-end security tool for mobile commerce. Such devices may include, but not limited to mobile phones, tablets etc.
Layer Two	**Mobile Commerce Language Security Layer**
	Language security layer relates to the elements dealing with mobile commerce security system development, such as software applications programming.
Layer Three	**Mobile Commerce Network Access Control Security Layer**
	Deals with wireless network access control security that provides access to mobile commerce network access. The main function of this security layer is to restrict users from accessing the wireless network.
Layer Four	**Mobile Commerce Access Management Security Layer**
	Controls authorized resource access, audits a users actions, provides non-repudiation of transaction and access control for a wireless web applications.
Layer Five	**Mobile Commerce Transaction Security Layer**
	Concerns mobile commerce application level transaction security functions that secure sensitive data throughout the transmission and logs all transactions.

The "Mobile Commerce Security Analysis (MCSA) model" as shown in Figure (2-3) below was adapted by adding mobile commerce security requirements measures into Wei et al (2006). The comprehensive measurement of actual mobile commerce transmission security structure includes ten aspects: "*authentication, integrity, confidentiality/ privacy, message authentication, non-repudiation, encryption, interoperability, vulnerability, information security, and hostility"* (Wei & Ozok, 2009).

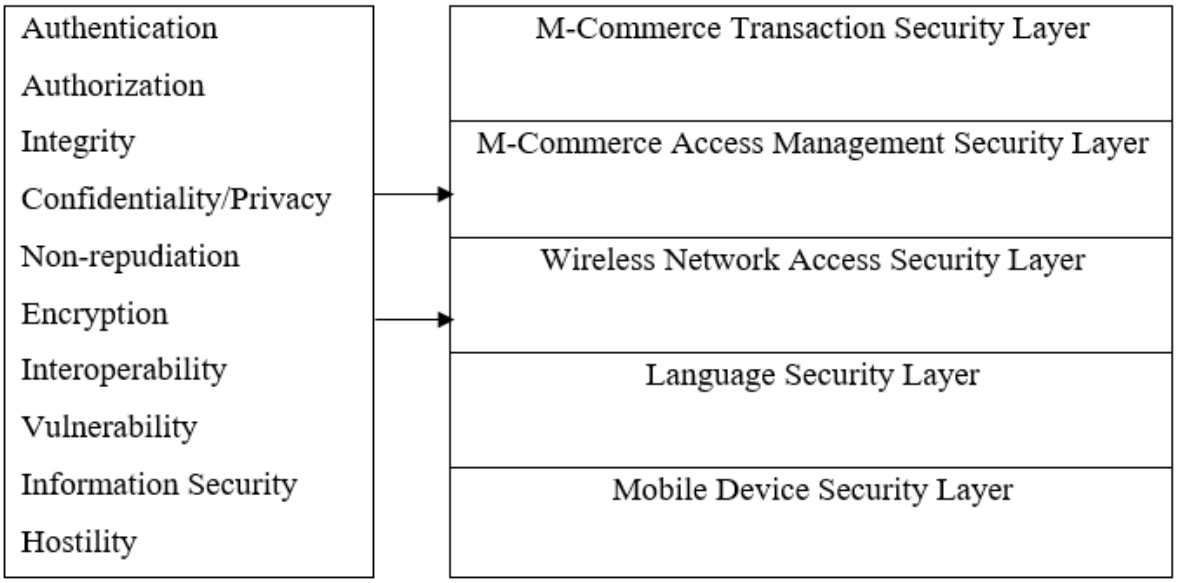

Figure 1-3: "M-Commerce Security Analysis (MCSA) Model" (Wei & Ozok, Development of a Mobile Commerce Security Analysis Method, 2009)

In this study only four aspects were adopted, since the inclusion of all ten aspects would prove very difficult to measure against mobile commerce customer satisfaction, while the aspects that were adopted include elements of the other aspects, since for example; Encryption methods are used to maintain Confidentiality/Privacy. The four aspects are as follows: “Authentication, Non-Repudiation, Integrity, Confidentiality/Privacy.”

- **Authentication**

Authentication is "any protocol or process that permits one entity to establish the identity of another entity." Through the realities of our physical world, the old authentication methods were done by recognizing special identifiers of the physical characteristics of human beings (Jadhao & Dole, 2013). Authentication and authorization are very closely tied, because authentication is essential to stop access for unauthorized parties (Spolaor, et al., 2016). There are three types of factor groups which are available to connect an individual with the established credentials. The development of authentication methods is shown in Figure (2-4) (Ometov, et al., 2018).

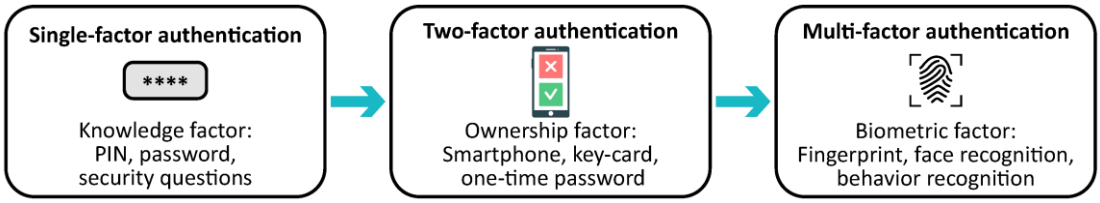

Figure 1-4: "Development of Authentication Methods from Single Factor Authentication (SFA) to Multi-Factor Authentication (MFA)" (Ometov, et al., 2018)

- **Non-Repudiation**

One of the fundamental security issues in electronic environments in Repudiation. It is common to have transaction disputes in the business world. Transacting parties want to see a fair settlement of disputes, which brings the need of non-repudiation services in their transactions. The motivation for non-repudiation services is not just the possibility that communicating parties may try to cheat each other. It is also the fact that no system is perfect, and that different and unexpected circumstances can arise in which two parties end up with different views of something that happened (Onieva, Zhou, & Lopez, 2008). Non-Repudiation "refers to a state of affairs where the purported maker of a statement will not be able to successfully

challenge the validity of the statement or contract." Repudiation is often seen in legal environment's in cases where the authenticity of a signature is challenged. In such an instance, the authenticity is being "repudiated" (Muliaro, Mwangi, & Kimani, 2013). Types of Non-Repudiation is as follows: "Non-Repudiation of Creation (ROC), Non-Repudiation of Delivery (NRD), Non-Repudiation of Knowledge (NRK), Non-Repudiation of Origin (NRO), Non-Repudiation of Receipt (ROR), Non-Repudiation of Sending (NRS), Non-Repudiation of Submission (NRSu), Non-Repudiation of Transport (NRT)" (Chen, Horng, & Liu, 2012).

- **Integrity**

Integrity in information security is usually defined "as the concept that information cannot be modified or tampered with without being noticed." Hence, It is about having an attacker unable to tamper or modify information without it being noticed by the owner of the information, and not about the concept of accessibility or security of the information. (Hansson, 2011). There are many exploits that damage the integrity of a mobile device by tampering with device (Zhang, Seifert, & Aciiçmez, 2014). The simple act of enabling users the ability to download applications exposes a threat to the security of the information on a mobile device. That is why these applications must be security critical by paying notice to the threats that may arise, and protect the integrity and secrecy of the data these applications have access to. There have been several documented cases of malware for mobile devices since 2004 (Muthukumaran, et al., 2011).

- **Confidentiality**

Confidentiality issues have been recognized by both industries and academia and the average user as one of the biggest concerns in mobile commerce. Having confidentiality and privacy of the gathered information that industries gather and collect on consumers is viewed as a right, both legally and ethically by consumers (Dai & Chen, 2015). Concerns in this issue encompasses four dimensions, which includes data collection, unauthorized access, unauthorized secondary use, and data accuracy, see Table (2-4) for more details (Zhang, Chen, & Lee, 2013).

Table 1-3: Dimensions of Information Confidentiality (Zhang, Chen, & Lee, 2013)

Dimension	***Explanation***
Data Collection	Concerns over excessive personal data collected and whether or not they are stored appropriately.
Unauthorized Access	Concerns over data access by unauthorized people.
Unauthorized secondary use	Concerns regarding the use of personal information for a purpose beyond its intended use.
Data accuracy	Concerns about whether individual data is adequately protect against accidental or intentional errors.

2.1.7 Customer Satisfaction

Satisfaction is a relational variable which has been studied in the context of mobile commerce, it implies fulfilling expectations as well as a positive affective state based on the result of maintaining the relation in the case of mobile commerce (San-Martin & Lopez-Catalan, 2013). Customer satisfaction has been examined extensively in marketing context and plays a strong role in a competitive environment while it also plays a considerable role in the decision-making for online shoppers and increasing repetitive purchases (Tandon, Kiran, & Sah, 2017).

To be satisfied, a customer has to be content with the product or service provided (Jiradilok, Malisuwan, Madan, & Sivaraks, 2014).

2.2 Previous Studies.

Sadi & Noordin (2011) study titled: "**Factors Influencing the adoption of Mobile Commerce: An Exploratory Analysis**", the purpose of this study aimed at identifying some factors that affect the adoption of mobile commerce in Malaysia using traditional technology models "Theory of Reason Action (TRA), Theory of Planned Behaviour (TPB), Technology Acceptance Model (TAM) and Diffusion Innovation Theory (DOI), an exploratory factor analysis was conducted on several factors that were measured against 349 respondents out of 600 questionnaires that were distributed. Findings found that all (13) factors were statistically significant and can affect the adoption of mobile commerce. Surprisingly the factor of security and privacy protection was not taken into consideration but the researchers did state in their conclusion that if security and privacy was a major concern in the adoption of services provided by mobile commerce, and did recommend consideration to secure systems be noted.

Chen, et. al. (2012) study titled: "**Strong Non-Repudiation based on certifcateless short signatures**", The purpose of this study is to consider certificateless signature (CLS) schemes for strong non-repudiation. The researchers exhibited that previous security models which ensure a user owning a unique key pair cannot guarantee a CLS scheme to achieve strong non-repudiation, the researchers fix existing security models, and introduced a new scheme (CLS-SNR) which offers strong non-repudiation.

Muliaro, et. al. (2013) study titled: "**Enhancing Personal Identification Number (PIN) Mechanism to Provide Non-Repudiation Through Use of Timestamps in Mobile Payment Systems**", purpose of this study was to enhance PIN to provide non-repudiation through the use of timestamps, the result of this study was an algorithm that will enhance PIN to provide non-repudiation through the use of timestamps.

Zhang, et. al. (2013) study titled: "**Mobile Commerce and Consumer Privacy Concerns**", this study attempts to identify the unique marketing context and features of mobile commerce as compared to e-commerce and to examine how consumer demographic characteristics affect their concern for information privacy, using the APCO model, the study conducted its research on 278 mobile device users in the U.S. it found varying degrees of impact in their demographic sample of concerns on privacy concerns which need to be addressed to ensure the future of mobile commerce. it recommends further research in studying consumer privacy concerns in the context of mobile commerce.

Singh & Giri (2014) study titled: "**Issues in Mobile E-Commerce: A Survey**", the purpose of this paper is to identify and discuss the issues that occur in mobile e-commerce which include technological issues and application issues pertaining to mobile commerce. Descriptive methodology was used through the use of secondary sources, concluding by listing the sensitive issues in mobile commerce and discussing what constitutes mobile commerce and the different kinds of services that is offered by it.

Jiradilok, et. al. (2014) study titled: "**The Impact of Customer Satisfaction on Online Purchasing: A Case Study Analysis in Thailand**", the purpose of which was to discover customer satisfaction and purchase intention impact on online purchasing through descriptive analytical research. The total sample size used in this research equalled 400 respondents which were divided into two groups those with experience and those without experience in purchasing online. Results show variables of appropriate pricing, website information quality, assurance, and empathy were statically significant, while variables of variety, responsibility were not significant.

Mirarab & Kenari (2014) study titled: "**Study of Secure Mobile Commerce, Challenges and Solutions**", its purpose is to focus on security issues in mobile commerce and analyse the security requirements and important vulnerabilities of mobile e-commerce, descriptive methodology was used to survey and introduce a mobile security architecture that is divided into four levels: network access security, provider domain security, user domain security, and application security, through the use of secondary sources. It concluded that due to the nature of mobile commerce being connected to wireless communication, it is required to deal with new security threats and new measures need to be developed as they are studied in due with the recommendations offered in this study.

Beyer (2014) study titled: "**Mobile Security: A literature Review**", purpose of which is to review literature related to mobile security specifically tablets and cell

phones that use Android, Apple, BackBerry OS, by using descriptive methodology and secondary sources. The study concluded that there is a distinct lack of literature regarding android security, and the number of articles written has risen but not much as would be expected considering the rise in mobile smartphone usage worldwide. It also concluded by list security issues and solutions, and stated that there is a clear opportunity for further scholarly research.

Ngoqo & Flowerday (2014) study titled: "**Exploring the Relationship Between Student Mobile Information Security Awareness and Behavioural Intent**", the purpose of this paper was to analyse the existing theories in the social sciences to gain an understanding of factors that contribute to student mobile device user's poor information security behaviour. It employed the "Kruger and Kearney" approach to measuring awareness, and the theory of planned behaviour to understand behavioural intent, using descriptive research methodology by observing student information security behavioural intent. It found that there is a poor security behaviour shown by student mobile device users, and found a huge gap between knowing and doing where users knowledge and awareness in information security does not result in safe behavioral practices, while also establishing a link between awareness and actual behavior.

Das & Khan (2015) study titled: "**Security Behaviours of Smartphone Users**", purpose of was to report on the information security behaviors of smartphone users as the title suggests in an affluent economy of the middle east. A model was developed using the FCC, ENISA that list malware, data leakage, and deliberate theft of

confidential information, with survey data from 500 smartphone users, their finding concluded that there is an overall low level of security behavior, the study attempted to apply an existing theory of information security behavior (the health belief model) to the relatively new domain of smartphone security, recommending to update its findings with the changes in security threats.

Ojha (2015) study titled: "**A Review of Security Issues in Mobile Agent-Based E-Commerce**", this study was undertaken to analyses security issues in mobile agents and the security requirements for e-commerce and available measures were listed to decrease the level of threats. Descriptive methodology was used to list security issues and security requirements using secondary sources, it concluded that a wide range of techniques do exist, none of them provide satisfactory solutions for the attacks. While recommending the need for a highly secure execution environment for mobile agents is a very basic demand for a successful deployment of mobile agent technology in e-commerce.

Shamsi & Afzi (2017) study titled: "**Security Threats to Mobile Commerce: Indian Perspective**", the purpose of this paper was to attempt to answer the research question of which is 'Is India ready for mobile commerce?' and identify the issues in the way of the future growth of mobile commerce, and understand the unique benefits and features of mobile commerce, while also analyzing various factors that affect it from security challenges. Research methodology followed content analysis of secondary sources such as firm disclosure data, and historical data analysis, company cases and sector reports. Its key findings were the widespread adoption of mobile devices and the

statement that there will be no mobile commerce without security of the underlying technologies, such barriers as lack of trust and awareness in mobile commerce and technology. Also the technical limitations and lack of a widely accepted standard can hinder the growth of mobile commerce in India.

ENISA (2017) Study titled: "**Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR**", the purpose of this study is to provide a meta-study on privacy and data protection in mobile apps by analyzing the features of the app development environment that impact privacy and security as well as discussing best practices and open ussies and gaps in the field. This study was supported by a group of experts in the field that conducted desk research and literature review, the main conclusions of which, were that guidance must be provided to app developers, there is a need for scalable methodologies and best practices, produced a Data Protection Impact Assessments (DPIs), stated the need for improving privacy and usability in the developer ecosystem, and addressed the entire mobile app ecosystem.

2.3 Distinctive Features of the Current Study from Previous Studies

Some comparisons as follows have been made to illustrate what distinguishes the current study from previous studies:

- This study investigates perceived information security factors on mobile commerce customers. These factors in information security are renewed as technology develops, which merits the research-ability of this subject.

- This study is distinguished by the location where it is applied; in Jordanian private universities – Amman.
- This study focuses on the impact of perceived information security variables on mobile commerce customer satisfaction, which other studies have not yet attempted to focus solely on this dimension.

Chapter 2 Study Methodology (Method and Procedures)

3.1 Introduction

This chapter exhibits several methods and procedures, which have been used to accomplish the objective of the study. It consists of a description of the study methodology, the study population and sample, the study tool and methods used to verify the validity and reliability, the study variables and the statistical treatments used in analyzing the study data in order to answer the study hypotheses, while in chapter five, the researcher discussed the statistical treatment that has been used in the analysis of the collected data.

3.2 Study Methodology

The researcher used descriptive analytical method to classify and analyze the data to describe the population of the study by recording the researcher of the events and presenting them and describing them through analytical descriptive tables. The tables are the primary data collected by the questionnaire and analyzed using the SPSS program. Which relate to the variables of the study, to reach real results and propose appropriate recommendations.

This study applied descriptive analytical method that depends on field scanning, aimed to investigate (The Impact of Perceived Information Security on Mobile Commerce Customer Satisfaction). Furthermore, the descriptive method was used to describe the characteristics of the sample of population allocated.

Collected data for the purpose of this study depended on the questionnaire developed by the researcher based upon several previous studies and

scientific reviews. The questionnaire was distributed to private university students in Amman, Jordan.

3.3 Study Population

The field of the study population is composed of all the students in the private universities, due to ease of access and ease of cooperation with those universities. The universities account to seven private universities in Amman – Jordan, as shown in Table (3-1) Population (Statistics: Ministry of Higher Education & Scientific Research, 2015-2016). which population data was pulled from. The combined population of all private universities in Amman, Jordan accounts for the study population. The student population was selected, because they are more likely to use mobile commerce. as previous literature shows that a high percentage of youth are avid users of the Internet and mobile apps, they are also quick to adopt new technologies.

Table 2-1: Private Universities in Amman, and their Establishment Year and Student

#	Private University	Establishment Year	Student Population
1	Princess Sumaya University for Technology	1990	2747
2	Al-Isra University	1991	5018
3	The Applied Science Private University	1991	6223
4	Al-Zaytoonah University of Jordan	1991	7376
5	The Petra University	1991	7192
6	The Amman Arab University	2001	2406
7	The Middle East University	2005	3158
Total Population of the Study			**34,120**

3.4 Study Sample

The sample of this study sample size consists of (300) which only (282) were retrieved (4) were lost and (14) were discarded due to missing data, out of (34120) students, who were chosen through simple random sampling due to the homogeneity of the population, who are studying at Jordanian private universities in Amman. The sample size was considered appropriately as it represents the total community according to (Sakaran & Bougie, 2013).

The sample was calculated through the following equation:

Sample Size = Z 2 * (p) * (1-p) /c 2

Z = Z value (90% confidence level)

P = Percentage picking a choice, (.5 used for the sample size needed)

C = confidence interval, (5)

3.5 Study Data Collection Tools

The data was obtained to achieve the objectives of this study were divided into the following:

- **Primary Source:** A questionnaire was prepared by the researcher to answer the study statements and hypothesis, for the purpose of understanding (The Impact of Perceived Information Security on Mobile Commerce Customer Satisfaction).
- **Secondary Source:** Books, journals, theses, articles, conferences, and worldwide web, were used to write theoretical framework of this thesis.

Table 2-2: The distribution of the paragraphs of the questionnaire and their number for each item

Variables	
Authentication	Questions from (01 to 06)
Non-Repudiation	Questions from (07 to 12)
Integrity	Questions from (13 to 17)
Confidentiality	Questions from (18 to 23)
Customer satisfaction	Questions from (24 to 32)

Both primary and secondary sources were used in this thesis. Furthermore, the data collected by using the questionnaire was constructed through the following three sections:

- **Section One:** This section collects demographic information that was collected with close-ended questions, through four factors which included: Gender, Age, Monthly Income (Including allowances, scholarships, wages and/or part time job fees), and Educational Level.
- **Section Two:** This section collects behavioral information on smartphone daily usage in university students, and the type of mobile-apps they download and use to better understand the concerns of the sample in regards to the type of usage.
- **Section Three:** This section measured the Perceived Information security over four aspects (Authentication, Non-Repudiation, Integrity, Confidentiality) (Wei & Ozok, 2009) (Wei, Liu, & Koong, 2006) (Suh & Han, 2003) and measured Mobile Commerce Customer Satisfaction as a single block adopted from (Jiradilok, Malisuwan, Madan, & Sivaraks, 2014).

The Questionnaire:

Initial items to measure various constructs are developed depending on prior researchers.

All variables will be measured by five-point Liker-type scale to tap into the students perceptions, ranging from value 1 (strongly disagree) to value 5 (strongly Agree) used through the questionnaire.

3.7 Tests for the Study Instrument

The researcher mentioned the reliability tests of the study tool in order to clarify its validity and validity in the tests, thus relying on the following tests:

- **Validation of study tool:**

The validity of the study tool is verified by presenting it to a group of faculty members concerned with the study variables. Their observations and notes were taken into account when constructing the study tool (questionnaire) and used to further modify it.

Reliability of the Study Test:

To measure the stability of the questionnaire and the level of its internal consistency of its values, the coefficient of Cronbach Alpha is used. Table (3-3) exhibits that.

Table 2-3: Internal consistency coefficients (Cronbach Alpha)

Variables	Stability Coefficient
Authentication	.887
Non-Repudiation	.890
Integrity	.700
Confidentiality	.810
Customer satisfaction	.830
Total	**.934**

Table (3-3) shows that the stability coefficients of the were higher than (70%). This indicates internal consistency between the paragraphs. (93.4 %), that is higher than (70%) indicating internal consistency among all paragraphs, which confirms the validity of the questionnaire in the hypothesis test (Khan & Abu-Salih, 1989).

3.9 Normal Distribution of Study Variables

To validate the absence study data from the statistical problems that could impact the study hypothesis, a normal distribution of variables used (Kolmogorov – Smirnov Z) test was obtained, Table (3-4) show the normality distribution for variable data, and therefore, it is found to be viable to measure the impact of perceived information security on mobile commerce customer satisfaction.

Table 2-4: Normal distribution of data

One-Sample Kolmogorov-Smirnov Test		
		Dependent
N		282
Normal Parameters[a,b]	Mean	4.2246
	Std. Deviation	.45740
Most Extreme Differences	Absolute	.167
	Positive	.167
	Negative	-.099-
Test Statistic		.167
Asymp. Sig. (2-tailed)		.000[c]
a. Test distribution is Normal.		
b. Calculated from data.		
c. Lilliefors Significance Correction.		

*The table shows that the distribution of data was followed by normal distribution.

Chapter 3 View the results and test hypotheses

This chapter examines The Effect of Variables. and the results derived from the statistical treatments and analyses conducted by the researcher concerning the characteristics of the sample by clarifying the statistical results of their answers, namely arithmetic means and standard deviations. Predetermined hypotheses and their statistical connotations.

4.1 Characteristics of Study Sample

In this study, the researcher dealt with some of the demographic variables of the sample in terms of (Gender, age, Monthly Income, Education Level,) as shown in Table (4-1) of the study as follows:

Table 3-1: Description of the study sample according to the demographic variables

Variables	Level/Category	Frequency	Percentage%
Gender	Male	167	59.2
	Female	115	40.8
Age	24 or Less	94	33.3
	Bt. 25-30	77	27.3
	Bt. 31-35	56	19.9
	36 or More	55	19.5
Monthly Income	Less than 300 JOD	203	72.0
	300 JOD or more	79	28.0
Education	High School	17	6.0
	Bachelor’s Degree	183	64.9
	Master’s Degree or Higher	57	20.2
	Other	25	8.9

Suprisngly a higher percentage of males answered the questionnaire. The researcher expecteded a higher percentage of women to answer the questionnaire since the represent a higher percentage of academic students in most universities, as stated by the statistics pulled from the Ministry of Higher Education & Scientific Research.

The behavioral variables of the sample in terms of (Smartphone Use, Shopping Usage, Transportation Usage, Social Media Usage, Gaming Usage) shown in Table (4-2) of the study was as follows:

Table 3-2: Description of the study sample according to the behavioural variables

Variables	Level/Category	Frequency	Percentage%
Smartphone Use	Daily	189	67.0
	Not Daily	93	33.0
Shopping Usage	Amazon	17	6.0
	Alibaba	9	3.2
	Souq.com	69	24.5
	Opensooq	109	38.7
	eBay	52	18.4
	Zara	3	1.1
	Fordeal	19	6.7
	Other	4	1.4
Transportation Usage	Uber	101	35.8
	Careem	140	49.6
	Lyft	2	0.7
	EasyTaxi	39	13.8

	SkyScanner	0	0.0
	Other	0	0.0
Social Media Usage	Facebook	282	100.0
	Instagram	282	100.0
	Twitter	190	67.4
	Snapchat	282	100.0
	YouTube	282	100.0
	Google+	124	44.0
	Pinterest	12	4.3
	Tumblr	1	0.4
	WhatsApp	282	100.0
	Other	282	100.0
Gaming Usage	PUBG Mobile	181	64.2
	Clash Royale	6	2.1
	Clash of Clans	90	31.9
	Subway Surfers	1	0.4
	My Talking Tom 2	1	0.4
	Other	3	1.1

Table (4-2) shows the sample description based on the behavioural variables of the sample.

Unsuprsingly the highest frequencies in mobile app usage were in social media, which refelect on the statistical impact of the variable of the study and elaborated further in the results of this study.

4.2 Paragraph compliance

The arithmetical averages and standard deviations of the sample responses of the study on the paragraphs:

Independent Variables:

1- Authentication

Table 3-3: The arithmetical averages and standard deviations of element (Authentication)

N	Paragraph	Mean	Standard Deviation	Rank	Approval Degree
1	The transactions I send are sent through to the real mobile application server to which I want to transmit.	4.13	.689	1	High
2	The transactions I receive are sent through to the real mobile application server to which I want to receive.	3.80	.862	4	High
3	Mobile applications verify my identity before sending me messages.	3.84	1.023	2	High
4	Mobile applications verify my identity before receiving messages from me.	3.76	1.040	6	High

5	Mobile applications verify my identity and protects me from unauthorized access.	3.80	.936	5	High
6	I use multi-factor authentication in mobile applications to verify my identity.	3.81	.997	3	High
	Total	**3.8570**	**.74471**		High

Table (4-3) shows that the computational circles of the sample responses ranged between (3.76- 4.13) with the highest computation (4.13) and the standard deviation (0.69) for paragraph (1) which is "The transactions I send are sent through to the real mobile application server to which I want to transmit.", The lowest mean (3.76) for paragraphs (4) which is "Mobile applications verify my identity before receiving messages from me".

2- Non-Repudiation

Table 3-4: The arithmetical averages and standard deviations of element (Non-Repudiation)

N	Paragraph	Mean	Standard Deviation	Rank	Approval Degree
7	Applications will not deny having participated in a transaction after processing it.	3.82	1.017	5	High
8	Mobile commerce applications will not deny having sent me a message.	3.88	.878	4	High

9	Mobile commerce applications will not deny having received a transaction from me.	3.93	.888	2	High
10	Mobile commerce applications provide me with some evidence to protect against its denial of having sent a message.	3.95	.893	1	High
11	Mobile commerce applications provide me with some evidence to protect against its denial of having received a transaction from me.	3.81	.971	6	High
12	Mobile commerce applications log all transaction activity for review by me.	3.92	.919	3	High
	Total	**3.8824**	**.74566**		High

"Table (4-4) shows that the computational circles of the sample responses ranged between (3.81- 3.95) with the highest computation (3.95) and the standard deviation (0.89) for paragraph (10) which is "Mobile commerce applications provide me with some evidence to protect against its denial of having sent a message.", The lowest mean (3.81) for paragraphs (11) which is " Mobile commerce applications provide me with some evidence to protect against its denial of having received a transaction from me. “.”

3- Integrity

Table 3-5: The arithmetical averages and standard deviations of element (Integrity)

N	Paragraph	Mean	Standard Deviation	Rank	Approval Degree
13	Mobile commerce applications check the information communicated with me for accuracy.	3.82	.954	5	High
14	Mobile commerce applications take steps to make sure that the information in transit is accurate.	3.82	.935	4	High
15	Mobile commerce applications take steps to make sure that the information in transit is not deleted.	4.47	.528	1	High
16	Mobile commerce application devote time and effort to verify the accuracy of the information in transit.	4.33	.615	3	High
17	Mobile commerce applications devote time and effort to verify that the information in transit is not deleted.	4.34	.684	2	High
	Total	**4.1560**	**.51433**		High

Table (4-5) shows that the computational circles of the sample responses ranged between (3.82- 4.47) with the highest computation (4.47) and the standard deviation (0.53) for paragraph (15) which is " Mobile commerce applications take steps to make

sure that the information in transit is not deleted.", The lowest mean (3.82) for paragraphs (13) which is “Mobile commerce applications check the information communicated with me for accuracy. “.

4- Confidentiality

Table 3-6: The arithmetical averages and standard deviations of element (Confidentiality)

N	Paragraph	Mean	Standard Deviation	Rank	Approval Degree
18	All mobile commerce apps must have a privacy policy.	4.38	.639	1	High
19	All communication through mobile commerce applications are restricted to the application and me.	4.34	.558	3	High
20	I am convinced that the mobile applications I use respect the confidentiality of the transaction received from me.	4.34	.546	2	High
21	Mobile commerce applications use some security control for confidentiality of transactions.	4.17	.694	6	High
22	Mobile commerce applications check all communication between the application and me for protection from wiretapping or eavesdropping.	4.20	.726	4	High
23	Mobile commerce applications will not use my personal information for	4.18	.853	5	High

	any purpose without my authorization.				
	Total	**4.2695**	**.48491**		High

Table (4-6) shows that the computational circles of the sample responses ranged between (4.17- 4.38) with the highest computation (4.38) and the standard deviation (0.64) for paragraph (18) which is " All mobile commerce apps must have a privacy policy.", The lowest mean (4.17) for paragraphs (21) which is " Mobile commerce applications use some security control for confidentiality of transactions".

5- Dependent Variable (Customer satisfaction)

Table 3-7: The arithmetical averages and standard deviations of element (Customer satisfaction)

N	Paragraph	Mean	standard deviation	Rank	Approval Degree
24	The mobile commerce apps that I use work whenever I need them.	4.34	.669	1	High
25	I find the prices of paid mobile commerce apps appropriate.	4.23	.608	5	High
26	The information I find in mobile commerce apps is interesting.	4.21	.696	6	High
27	I find the quality of the mobile commerce apps I use is satisfactory.	4.30	.595	2	High
28	I sense tangible benefits in mobile commerce apps.	4.17	.657	7	High

29	I use mobile commerce apps to execute most of the commercial transactions I need.	4.27	.569	4	High
30	Mobile commerce apps I use set clear responsibilities to follow through.	4.30	.635	3	High
31	I find confidence in the mobile applications I use.	4.09	.922	9	High
32	I receive apologies/compensation for unsatisfactory experiences in mobile commerce apps.	4.12	.879	8	High
	Total	**4.2246**	**.45740**		High

Table (4-7) shows that the computational circles of the sample responses ranged between (4.09- 4.34) with the highest computation (4.34) and the standard deviation (0.67) for paragraph (24) which is “The mobile commerce apps that I use work whenever I need them.", The lowest mean (4.09) for paragraphs (31) which is " I find confidence in the mobile applications I use".

Descriptive analysis of the independent variable

Table 3-8: Descriptive analysis of the independent variable (Information Security)

	Element	**Mean**	**Standard Deviation**	**Approval Degree**
Information Security	Authentication	3.8570	.74471	High
	Non-Repudiation	3.8824	.74566	High
	Integrity	4.1560	.51433	High
	Confidentiality	4.2695	.48491	High

	Total	**4.0412**	**.51482**	**High**

Table (4-8) shows that the computational circles of the sample responses ranged between (3.86- 4.27) with the highest computation (4.27) and the standard deviation (0.48) for Element (Confidentiality) with high degree, then the element (Integrity) Where it reached the arithmetic mean of the element (4.16) and the standard deviation (0.51), then the element (Non-Repudiation) Where it reached the arithmetic mean of the element (3.88) and the standard deviation (0.75), Finally The lowest mean (3.86) for Element (Authentication) and it the standard deviation (0.74).

4.5 Test hypotheses

- **The main hypothesis**

H01: There is a statistically positive impact of Perceived Information Security on Mobile Commerce Customer Satisfaction in Jordanian Private University Students, at the level of significance ($\alpha \leq 0.05$).

A simple and multiple regression analysis was carried out to determine the effect of perceived information security on mobile commerce customer satisfaction at the level of significance ($\alpha \leq 0.05$).

Table 3-9: b (Model Summary)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.733[a]	.538	.531	.31318

Table (4-9) shows that the value of the correlation coefficient of the variable (Perceived Information Security) and the variable (customer satisfaction) was % 73.3. The value of the coefficient of determination (R2) is 0.538, so % 53.8 of the total variance is explained by the model and the rest is explained by other factors.

Multiple regression test:

Table 3-10: Analysis of variance (ANOVA)

Model		Sum of Square	Df	Mean Square	F	Sig.
1	**Regression**	31.619	4	7.905	80.593	.000[b]
	Residual	27.169	277	.098		
	Total	58.789	281			

Table (4-10) shows that the value of F is (80.593) and the statistical significance level is (0.00) and thus is less than (0.05). Thus, hypothesis is accepted. There is impact of Perceived Information Security at the significant level (a ≤ 0.05) on customer satisfaction.

Multivariate regression coefficients:

Table 3-11: Table of Transactions a (Coefficient)

Element	B	Std. Error	Beta	T	Sig.
(Constant)	1.136	.181		6.268	.000
Authentication	.066	.051	.107	1.292	.197
Non-Repudiation	.032	.053	.052	.602	.548
Integrity	.027	.051	.031	.533	.595
Confidentiality	.608	.046	.645	13.223	.000

Table (4-11) shows that after the variable (Confidentiality), that significance was (0.000) less than (0.05), indicating that Confidentiality has a statistically significant effect on customer satisfaction, and the rest of the element have a positive effect that is apparent, but not statistically significant.

- **The results of the first sub-hypothesis test**

H01.1: There is a statistically positive impact of Authentication on Mobile Commerce Customer Satisfaction in Jordanian Private University Students at the level of significance ($\alpha \leq 0.05$).

A simple and multiple regression analysis was carried out to determine the effect of Authentication on customer satisfaction at the level of significance ($\alpha \leq 0.05$).

Table 3-12: b (Model Summary)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.390[a]	.152	.149	.42199

Table (4-12) shows that the value of the correlation coefficient of the variable (Authentication) and the variable (customer satisfaction) was %39.0. The value of the coefficient of determination (R2) is 0.152, so %15.2 of the total variance is explained by the model and the rest is explained by other factors.

Multiple regression test:

Table 3-13: Analysis of variance (ANOVA)

Model		Sum of Square	Df	Mean Square	F	Sig.
1	**Regression**	8.927	1	8.927	50.131	.000[b]
	Residual	49.861	280	.178		
	Total	58.789	281			

Table (4-13) shows that the value of F is (50.131) and the statistical significance level is (0.00) and thus is less than (0.05). Thus, the hypothesis is accepted. There is impact of Authentication at the significant level ($a \leq 0.05$) on customer satisfaction.

- **The results of the second sub-hypothesis test**

H01.2: There is a statistically positive impact of Non-Repudiation on Mobile Commerce Customer Satisfaction in Jordanian Private University Students at the level of significance ($\alpha \leq 0.05$).

A simple and multiple regression analysis was carried out to determine the effect of Non-Repudiation on customer satisfaction at the level of significance ($\alpha \leq 0.05$).

Table 3-14: b (Model Summary)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.383[a]	.147	.144	.42323

Table (4-14) shows that the value of the correlation coefficient of the variable (Non-Repudiation) and the variable (customer satisfaction) was %38.3. The value of the

coefficient of determination (R2) is 0.147, so %14.7 of the total variance is explained by the model and the rest is explained by other factors.

Multiple regression test:

Table 3-15: Analysis of variance (ANOVA)

Model		Sum of Square	Df	Mean Square	F	Sig.
1	**Regression**	8.633	1	8.633	48.196	.000[b]
	Residual	50.155	280	.179		
	Total	58.789	281			

Table (4-15) shows that the value of F is (48.196) and the statistical significance level is (0.00) and thus is less than (0.05). Thus, hypothesis is accepted. There is impact of Non-Repudiation at the significant level ($a \leq 0.05$) on customer satisfaction.

- **The results of the Third sub-hypothesis test**

H01.2: There is a statistically positive impact of Integrity on Mobile Commerce Customer Satisfaction in Jordanian Private University Students at the level of significance ($\alpha \leq 0.05$).

A simple and multiple regression analysis was carried out to determine the effect of Integrity on customer satisfaction at the level of significance ($\alpha \leq 0.05$).

Table 3-16: b (Model Summary)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.474[a]	.224	.222	.40353

Table (4-16) shows that the value of the correlation coefficient of the variable (Integrity) and the variable (customer satisfaction) was %47.4. The value of the coefficient of determination (R2) is 0.224, so %22.4 of the total variance is explained by the model and the rest is explained by other factors.

Multiple regression test:

Table 3-17: Analysis of variance (ANOVA)

Model		Sum of Square	Df	Mean Square	F	Sig.
1	**Regression**	13.195	1	13.195	81.032	.000[b]
	Residual	45.594	280	.163		
	Total	58.789	281			

Table (4-17) shows that the value of F is (81.032) and the statistical significance level is (0.00) and thus is less than (0.05). Thus, hypothesis is accepted. There is impact of Integrity at the significant level (a ≤ 0.05) on customer satisfaction.

- **The results of the Forth sub-hypothesis test**

H01.2: There is a statistically positive impact of Confidentiality on Mobile Commerce Customer Satisfaction in Jordanian Private University Students at the level of significance (α ≤ 0.05).

A simple and multiple regression analysis was carried out to determine the effect of Confidentiality on customer satisfaction at the level of significance (α≤0.05).

Table 3-18: b (Model Summary)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.716[a]	.512	.511	.31994

Table (4-18) shows that the value of the correlation coefficient of the variable (Confidentiality) and the variable (customer satisfaction) was %71.6. The value of the coefficient of determination (R2) is 0.512, so %51.2 of the total variance is explained by the model and the rest is explained by other factors.

Multiple regression test:

Table 3-19: Analysis of variance (ANOVA)

Model		Sum of Square	Df	Mean Square	F	Sig.
1	**Regression**	30.128	1	30.128	294.333	.000[b]
	Residual	28.661	280	.102		
	Total	58.789	281			

Table (4-19) shows that the value of F is (294.333) and the statistical significance level is (0.00) and thus is less than (0.05). Thus, hypothesis is accepted. There is impact of Confidentiality at the significant level ($a \leq 0.05$) on customer satisfaction.

Table 3-20: Study Model Variables Impact

Hypothesis No	Variables		Support/not
Ho1	**Perceived Information Security** ⇨	**customer satisfaction**	Supported
H01.1	**Authentication** ⇨	**customer satisfaction**	Supported
H01.2	**Non-Repudiation** ⇨	**customer satisfaction**	Supported
H01.3	**Intgrity** ⇨	**customer satisfaction**	Supported
H01.4	**Confidentiality** ⇨	**customer satisfaction**	Supported

As shown in Table (4-2) all the study model independent variables are supported to have impact on mobile customer satisfaction.

Chapter 4 Discussion of Results and recommendations

5.1 Results

The results of this study indicate that here is an impact of Perceived Information Security at the significant level (a ≤ 0.05) on mobile commerce customer satisfaction in Jordanian private universities in Amman. They also show that after the variable (Confidentiality), that significance was (0.000) less than (0.05), indicating that Confidentiality has a statistically significant effect on mobile commerce customer satisfaction, and the rest of the element have a positive effect that is apparent, but not statistically significant. Finally, there are impacts of (Authentication, Non-Repudiation, Integrity, Confidentiality) at the significant level (a ≤ 0.05) on mobile commerce customer satisfaction.

5.2 Similarities and Differences to Other Studies

Sadi & Noordin (2011) study titled: "**Factors Influencing the adoption of Mobile Commerce: An Exploratory Analysis**", Did not take in directly security as a factor since it already had it noted as a definite factor that affects the adoption of mobile commerce, which is indirectly linked to satisfaction.

Shamsi & Afzi (2017) study titled: "**Security Threats to Mobile Commerce: Indian Perspective**", agreed with the findings of the current study that non-repudiation, confidentiality and authentication were major threats to mobile commerce and must be handled to reach satisfied customers who would adopt the technology.

5.3 Recommendations

1. Ensuring that information security and its perception by the customer in mobile commerce is a continuous work and not a project or task that ends with the application of security solutions.
2. Take advantage of past experiences and security incidents and work on fulfilling the gaps and weaknesses in security to better satisfy customer satisfaction.
3. The need for a comprehensive study that prepares a full-proof security architecture that takes into account current security architectures and develop them.
4. Ensuring that information security is everyone's responsibility, depending on the nature of its work, both users and developers.

References

Beyer, C. (2014). Mobile Security: A Literature Review. *International Journal of Computer Applications (0975 - 8887)*.

Boxall, A. (2016, October 7). *There are 12 million mobile developers worldwide, and nearly half develop for Android first*. Retrieved from Business of Apps: http://www.businessofapps.com/12-million-mobile-developers-worldwide-nearly-half-develop-android-first/

Budzak, D. (2016). Information Security: the People Issue. *Business Information Review, Vol. 33*(No. 2), 76-80.

Charland, A., & LeRoux, B. (2011). Mobile Application Development: Web Vs Native. *Communications of the ACM CACM*, 49-53.

Chen, Y.-C., Horng, G., & Liu, C.-L. (2012). Strong Non-Repudiation Based on Certificateless Short Signatures. *IET Information Security, Vol. 7*(No. 3), 253-283.

Cherdantseva, Y., & Hilton, J. (2013). *Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals.* Cardiff University, Department of Informatics and Systems Engineering. Swindon: IGI Global Publishing.

Dai, H., & Chen, Y. (2015). Effects of Exchange Benefits, Security Concerns and Situational Privacy Concerns on Moile Commerce Adoption. *Journal of International Technology and Information Management, Vol. 24*(No. 3), 41-56.

Doherty, A. (2018, October 15). *Highlights From Dark Reading's 2018 Strategic Security Survey*. Retrieved from UBM. Technology Group: https://tech.ubm.com/news/highlights-dark-reading%E2%80%99s-2018-strategic-security-survey

Douglas, K. H., Wojcik, B. W., & Thompson, J. R. (2012). Is There an App for That? *Journal of Special Education Technology*, 59-70.

Elmore, T. (2014, September 18). *Nomophobia: A Rising Trend in Students*. Retrieved from Psychology Today: https://www.psychologytoday.com/us/blog/artificial-maturity/201409/nomophobia-rising-trend-in-students

ENISA. (2017). *Privacy and Data Protection in Mobile Applications.* Heraklion: European Union Agency For Network and Information Security.

Fornell, C., Johnson, M. D., Anderson, E. W., Cha, J., & Bryant, B. E. (1996). The American Customer Satisfaction Index: Nature, Purpose, and Findings. *Journal of Marketing*, 7-18.

Giri, M., & Singh, S. (2014). Issues in Mobile E-Commerce: A Survey. *International Journal of Computer and Information Technologies, Vol. 5*(No. 4), 5066-5070.

Hansson, F. (2011). *System Integrity for Smartphones.* Master Thesis, Linköping University, Linköping.

Hung, D.-L., Rau, P.-L. P., Salvendy, G., & Shang, X.-L. (2008). Perception of Information Security and its Implications for Mobile Phone. *Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting* (pp. 1650-1654). New York: Santa Monica, CA : Human Factors & Ergonomics Society.

Jadhao, P., & Dole, L. (2013). Survey on Authentication Password Techniques. *International Journal of Soft Computing and Engineering, Vol-3*(Issue-2), 67-68.

Jiradilok, T., Malisuwan, S., Madan, N., & Sivaraks, J. (2014). The Impact of Customer Satisfaction on Online Purchasing: A Case Study Analysis in Thailand. *Journal of Economics, Business and Management, Vol. 2*(No. 1), 5-11.

Khan, A., & Abu-Salih, M. (1989). Characterizations of probability distributions by conditional expectation of order statistics. *Metron, 47*, 171-181.

Marufu, A. M. (2013). An M-Commerce Security Framework for ICt4D Contexts. *Southern Africa Telecommunication Networks and Application Conference* . Stellenbosch, Western Cape: SATNAC.

Muliaro, J., Mwangi, I., & Kimani, S. (2013). Enhancing Personal Identification Number (PIN) Mechanism to Provide Non-Repudiation Through Use of Timestamps in Mobile Payment Systems. *International Journal of Advanced Research in Computer Science, Vol. 4*(No. 10), 1-11.

Muthukumaran, D., Joshua, S., Hassan, M., Sawani, A., Rao, V., & Jaeger, T. (2011). Protecting the integrity of trusted applications in mobile phone systems. *Security and Communication Networks, vol. 4*(no. 6), 633-650.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 47-66.

NATO. (2016, October). *Cybersecurity A Generic Reference Curriculum.* Retrieved from North Atlantic Treaty Organization: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf

Nield, D. (2018, Jaunary 04). *All the Ways Your Smartphone and Its Apps Can Track You*. Retrieved from GIZMODO: https://gizmodo.com/all-the-ways-your-smartphone-and-its-apps-can-track-you-1821213704

Ojha, A. C. (2015). A Review of Security Issues in Mobile Agent-Based E-Commerce. *The IUP Journal of Information Technology, Vol. 11*(No. 1), 53-59.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography, 2*(1), 1-31.

Onieva, J. E., Zhou, J., & Lopez, J. (2008). Multi-Party Non-Repudiation: A Survey. *ACM Computing Surveys, Vol. 5*, 1-46.

Said, S., & Noordin, M. (201). Factors Influencing the Adoption of M-Commerce: An Exploratory Analysis. *Proceedings of the 2011 International Conference on Industrial Engineering and Operations Management*, (pp. 22-24). Kuala Lumpur.

Sakaran, U., & Bougie, R. (2013). *Research Methods for Business: A Skill Building Approach* (6th ed ed.). Chichester (West Sussex): Wiley.

San-Martin, S., & Lopez-Catalan, B. (2013). How can a mobile vendor get satisfied customers? *Industrial Management & Data Systems, Vol. 113*(No. 2), 157-170.

Shamsi, K., & Afzal, M. (2017). Security Threats to M-Commerce: Indian Perspective. *International Journal of Engineering Inventions, Vol. 6*(No. 1), 56-60.

Shea, M. R. (2015, August). *Mobile Security: A Balance Between Encryption, Privacy, And Forensics.* Master Theses, Utica University, Utica.

Spolaor, R., Li, Q., Monaro, M., Conti, M., Gamberini, L., & Sartori, G. (2016). Biometric Authenticcation Methods on Smartphones: A Survey. *PsychNology Journal, Vol-14*, 87-98.

Stanoevska-Slabeva, K. (2003). Towards a reference model for m-commerce applications. *Proceedings of the 11th European Conference on Information Systems* (pp. 16-21). Naples: ECIS.

Statistics: Ministry of Higher Education & Scientific Research. (2015-2016). *The Annual Statistical Report on Higher Education in Jordan for the year*. Retrieved 2018, from The Hashemite Kingdom of Jordan Ministry of Higher Education & Scientific Research Web Site: http://www.mohe.gov.jo/en/pages/Statistics.aspx

Suh, B., & Han, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce, Vol. 7*(No. 3), 135-161.

Tandon, U., Kiran, R., & Sah, A. (2017). Analyzing customer satisfaction: users perspective towards online shopping. *Nanki Business Review International, Vol. 8*(No. 3), 266-288.

The Statistics Portal. (2018). *Number of smartphone users worldwide from 2014 to 2020 (in billions)*. Retrieved from Statistica: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A Risk Assessment Method for Smartphones. *IFIP International Information Security Conference* (pp. 443-456). Berlin: Springer, Berlin, Heidelberg.

Wei, J., & Ozok, A. (2009). Development of a Mobile Commerce Security Analysis Method. *Jounrla of Information Privacy & Security*, 28-48.

Wei, J., Liu, L. C., & Koong, K. S. (2006). An onion ring framework for developing and assessing mobile commerce security. *Int. J. Mobile Communications*, 128-142.

Weiss, G. M. (2013, Jaunary 4). *Your Smartphone Knows You Better Than You Know Yourself*. Retrieved from Inside Science: https://www.insidescience.org/news/your-smartphone-knows-you-better-you-know-yourself

Wushishi, U. J., & Ogundiya, A. O. (2014). Mobile Commerce and Security Issues. *International Journal of Scientific Research Engineering & Technology*, 739-741.

Xu, H., & Yang, J. (2012). Do M-Commerce User's Expectations Reflect Reality? *International Journal of Elecronic Business Management*, 322-331.

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile Commerce and Consumer Privacy Concerns. *The Journal of Computer Information Systems, Vol. 53*(No. 4), 31-38.

Zhang, X., Seifert, J.-P., & Aciiçmez, O. (2014). Design and Implementation of Efficient Integrity Protection for Open Mobile Platforms. *IEEE Transactions on Mobile Computing, Vol. 13*(no. 1), 188-201.

Appendix

Appendix (1) The Study Questionnaire

Scientific Research Questionnaire

Dear Participant,

The researcher is currently conducting a scientific study intended to identify the**:" The Impact of Information Security on Mobile Commerce Customer Satisfaction: A field Study in Jordanian Private Universities in Amman".**

The Purpose of this study is to obtain a master's degree in E-Business, your assistance in answering the study questionnaire means a lot to us and will add value to our study. It will be used only for academic purpose and will not be used outside the scope of this scientific research.

I would appreciate your kind assistance very much to answer the following questions that number 42, which will take you approx. 10 minutes to answer.

Thank you very much.

Supervisor
Prof. Ahmad Al-Sukkar

Researcher
Aidmar Hasan Biltawi

No	Section I			
	Personal Information			
1	**Gender**			
	Female	☐	Male	☐
2	**Age**			
	24 or less	☐	25-30	☐
	31-35	☐	36 or more	☐
3	**Monthly Income (Including allowances, scholarships, wages and/or part time job fees)**			
	Less Than 300 JOD	☐	More than 300 JOD	☐
4	**Education Level**			
	High School	☐	Bachelor	☐
	Masters or Higher	☐	Other:…….	☐

No	Section II			
1	**Do you use a Smartphone?**			
	Daily	☐	Not Daily	☐
	Which of the following applications do you use? (please note you can tick (√) more than one checkbox and add a selection)			
2	**Shopping Applications Usage**			
	Amazon	☐	Alibaba	☐
	Souq.com	☐	Opensooq	☐
	Modansia	☐	Jollychic	☐
	eBay	☐	Zara	☐
	Fordeal	☐	Other:……	
3	**Transportation Applications Usage**			
	Uber	☐	Careem	☐
	Lyft	☐	EasyTaxi	☐
	SkyScanner	☐	Other:……	
4	**Social Media Applications Usage**			
	Facebook	☐	Instagram	☐
	Twitter	☐	Snapchat	☐
	YouTube	☐	Google+	☐
	Pinterest	☐	Tumblr	☐
	WhatsApp	☐	Other:……	
5	**Game Applications Usage**			
	PUBG Mobile	☐	Clash Royale	☐
	Clash of Clans	☐	Subway Surfers	☐
	My Talking Tom 2	☐	Other:……	

Section III						
No.	**Field**	Strongly Disagree	Disagree	Don't Know	Agree	Strongly Agree
Information Security						
Authentication: The process of verifying the identity or other attributes of an entity.						
1	The transactions I send are sent through to the real mobile application server to which I want to transmit.					
2	The transactions I receive are sent through to the real mobile application server to which I want to receive.					
3	Mobile applications verify my identity before sending me messages.					
4	Mobile applications verify my identity before receiving messages from me.					
5	Mobile applications verify my identity and protects me from unauthorized access.					
6	I use multi-factor authentication in mobile applications to verify my identity.					
Non-Repudiation: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information						
7	Applications will not deny having participated in a transaction after processing it.					
8	Mobile commerce applications will not deny having sent me a message.					
9	Mobile commerce applications will not deny having received a transaction from me.					
10	Mobile commerce applications provide me with some evidence to protect against its denial of having sent a message.					
11	Mobile commerce applications provide me with some evidence to protect					

	against its denial of having received a transaction from me.					
12	Mobile commerce applications log all transaction activity for review by me.					
Integrity: Ensures that information has not been modified or altered during a transmission						
13	Mobile commerce applications check the information communicated with me for accuracy.					
14	Mobile commerce applications take steps to make sure that the information in transit is accurate.					
15	Mobile commerce applications take steps to make sure that the information in transit is not deleted.					
16	Mobile commerce application devote time and effort to verify the accuracy of the information in transit.					
17	Mobile commerce applications devote time and effort to verify that the information in transit is not deleted.					
Confidentiality: The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information						
18	All mobile commerce apps must have a privacy policy.					
19	All communication through mobile commerce applications are restricted to the application and me.					
20	I am convinced that the mobile applications I use respect the confidentiality of the transaction received from me.					
21	Mobile commerce applications use some security control for confidentiality of transactions.					
22	Mobile commerce applications check all communication between the application and me for protection from wiretapping or eavesdropping.					
23	Mobile commerce					

	applications will not use my personal information for any purpose without my authorization.					
Mobile Commerce Customer Satisfaction						
Customer Satisfaction: Customer satisfaction is when products and services meet the expectation of the consumers						
24	The mobile commerce apps that I use work whenever I need them.					
25	I find the prices of paid mobile commerce apps appropriate.					
26	The information I find in mobile commerce apps is interesting.					
27	I find the quality of the mobile commerce apps I use is satisfactory.					
28	I sense tangible benefits in mobile commerce apps.					
29	I use mobile commerce apps to execute most of the commercial transactions I need.					
30	Mobile commerce apps I use set clear responsibilities to follow through.					
31	I find confidence in the mobile applications I use.					
32	I receive apologies/compensation for unsatisfactory experiences in mobile commerce apps.					

Appendix (2) Questionnaire Arbitrators

Questionnaire Arbitrators Panel

NO.	Professor Name	University
1	Prof. Adel Bino	Jordan University
2	Prof. Khalid Abu Ghanam	Jedah University
3	Prof. Mefleh Al-Jarah	Amman Arab University
4	Prof. Mahmoud Al-Dalahmeh	Jordan University
5	Prof. Mohammad Al-Adaileh	Middle East University
6	Prof. Ahmad Ali Saleh	Middle East University
7	Prof. Sameer Al-Jabali	Middle East University

Appendix (3) Letter of Mission Facilitation

جـامـعـة الـشـرق الأوسـط
MEU MIDDLE EAST UNIVERSITY
Amman - Jordan

مكتب رئيس الجامعة
President's Office

الرقم: د ر/خ/502/26
التاريخ: 2019/01/02

لمن يهمة الامر

تحية طيبة وبعد،

فلغايات توفير وربط أسس التعاون مع خدمة المجتمع المحلي، نرجو التكرم بالموافقة على تقديم التسهيلات الممكنة للطالب ايدمر حسن بلتاوي، ورقمه الجامعي(401610114)، تخصص أعمال إلكترونية/ مقترح رسالة، والذي يقوم فيه بإعداد دراسة بحثية أكاديمية للجامعات الأردنية الخاصة؛ حيث أن المعلومات التي سيتم الحصول عليها سوف تستخدم في أغراض البحث العلمي وبصورة سرية.

وتفضلوا بقبول فائق الاحترام...

رئيس الجامعة

أ.د. محمد محمود الحيلة

MEU President's Office MIDDLE EAST UNIVERSITY

info@meu.edu.jo بريد الكتروني ص.ب 383 عمان 11831 الاردن (00962 6) 4129613 فاكس (00962 6) 4790222 هاتف
Tel. (00962 6) 4790222 Fax. (00962 6) 4129613 P.O.Box 383 Amman 11831 Jordan e-mail:info@meu.edu.jo www.meu.edu.jo

جـامـعـة الـشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

مكتب رئيس الجامعة
President's Office

الرقم: د ر/خ/319/5
التاريخ: 2018/11/26

لمن يهمه الامر

تحية طيبة وبعد،

أرجو التكرم بالإيعاز لمن يلزم بتسهيل مهمة الطالب **ايدمر حسن بلتاوي**، وهي أحد طلبة جامعة الشرق الأوسط / تخصص أعمال إلكترونية / كلية الأعمال، ورقمه الجامعي (**401610114**)، والذي يقوم بإعداد دراسة بحثية أكاديمية للجامعات الخاصة.

راجيًا الإيعاز لمن يلزم بتقديم كل التسهيلات الممكنة للطالب، علماً بأن المعلومات التي سيحصل عليها ستبقى سرية ولن تستخدم إلا لأغراض البحث العلمي فقط.

شاكرين ومقدرين لكم حسن تعاونكم واهتمامكم.

وتفضلوا بقبول فائق الاحترام...

رئيس الجامعة
25.11.2018
أ.د. محمد محمود الحيلة