Macrothink Institute™

**Business and Economic Research**
ISSN 2162-4860
2017, Vol. 7, No. 2

# Positive and Negative Effects of Using Electronic Banking on Customers and Small Entrepreneurs: An Exploratory Study in the Western Region of Saudi Arabia

Dr. Nayef Salah Ghamri (Corresponding author)

Faculty of Economics and Administration King Abdulaziz University

Jeddah, Saudi Arabia

Tel: 966-566-108-822 E-mail: nayef.alghamri@gmail.com

Received: September 20, 2017 Accepted: October 7, 2017

doi:10.5296/ber.v7i2.11999 URL: https://doi.org/10.5296/ber.v7i2.11999

**Abstract**

Currently, the exchange of digital knowledge is not confined to a place or time. Knowledge is being shared among peoples all over the world regardless of the geographical and political boundaries. Technology, from the time of its existence, has contributed in changing many people's rooted concepts that they have been accustomed to in their lives. While technology has positively contributed in shortening the time and distances among nations, it has also created some negative consequences such as the difficulty of protecting the individual's privacy. In the era of widespread technology, new types of money thefts have emerged. These thefts do not include breaking into houses and banks but rather, Internet piracy. This is one of the modern types of thefts, which is represented in many forms such as identity theft, transferring money from one bank account into another, and the thefts of sensitive and confidential information. Therefore, information technology has an important role to play in our life, and it became one of our priorities. This research study focuses on assessing the risks related to the theft of the information of the clients of the commercial banks and even considering the level of security and theft prevention of such information as one of the key factors of quality that most banks show as one of their competitive advantages which they are trying to maintain.

**Keywords:** Electronic banking; hacking, internet security, Saudi Arabia

This research consists of five parts:

1. Part I: Addresses the problem of the research study, its objectives, significance, and hypotheses.
2. Part II: Tackles the theoretical framework of the research and previous studies.
3. Part III: Presents the research methodology, data collection techniques, data verification, and statistical methods as well as the procedures used in the research.
4. Part IV: Presents the analysis of the results of the field study and tests the validity of the hypotheses.
5. Part V: Focuses on the results and recommendations of the research study.

## 1. First, the General Framework

### *1.1 Introduction*

Information is the feature of our era where the internet transfers information everywhere, to civil institutions and governmental organizations as well. Information has been used since Romans time, and the military information was one of the fundamental pillars of victory.

Technology is a Greek term which is originally derived from the two words "*tecknNe*" which means technique or art and the word *logos* which means science and study. Idiomatically, technology is defined as a set of applied systems, rules and working methods that settle for the application of the data used for innovative research and studies in the field of production and services. It represents a range of tools and techniques used by individuals in various aspects of their scientific career. Therefore, it is a texture composed of equipment and human knowledge (Al Fateh et al., 2011).

With the emergence of modern technology and the change in cultural thoughts towards economic prosperity, countries around the world became interested in the information in general and financial and investment information in particular, to which computers and the Internet played a major role in its readiness and ease of use. Thus, confidentiality of information is recently associated with the Internet and computers. Confidentiality of information captures the attention of researchers, officials, legislators and ordinary individuals alike. Academically, confidentiality and security of information is the science that explores the theories and strategies that provide protection of information against risks and activities that threaten it. Technically, confidentiality and security of information include the means, tools and procedures necessary to ensure the protection of information against internal and external threats. Legally, confidentiality of information is the study of measures for protection and safety of the content, its availability, and its control (Zuhairi, 2010). The term “confidentiality of information” can be defined as the science which provides protection for the information against risks and violations through providing the available necessary tools and means to protect information against internal and external risks. It also provides accurate standards and measures to prevent access of unauthorized individuals to sensitive information in order to ensure the authenticity and validity of communications. The confidentiality of information is an old concept. However, it began to be intensively implemented since the evolution of technology in general and the Internet in particular, to keep the secrecy of

information (Wikipedia confidentiality of information, 2015). With the widespread of information culture and cognitive society, computer illiteracy emerged in the form of individuals' incapability of dealing with means of communications, computers, and the Internet even though they were highly educated individuals.

*1.2 Second, the Theoretical Framework and Previous Studies*

The effect of electronic banks (e-banks) was huge on our daily life style. Electronic banks enabled individuals to benefit from the provided unlimited features. In addition, e-banks enabled their customers and small entrepreneurs to benefit from the provided electronic services with all possible and convenient means for accessing the service. In the e-banking era, customers neither need to queue up in front of the traditional banks to open their doors in order to withdraw money from their accounts, nor do they need to rush the time to make a transaction before the banks close. The electronic services are not associated with a particular place or time, as they enable customers and small entrepreneurs to process transactions anywhere in the world and at any time quickly surpassing every human imagination.

Furthermore, the association between mobile phones and the Internet became the most wonderful aspects of the digital age, and it became extremely difficult to stop the use of computers and the Internet in the present time. However, computers and smart phones may contain sensitive and important information for individuals and organizations, which has generated new approaches and practices to ensure the availability of data and information on these devices. Consequently, security bugs were exploited with or without the users' knowledge to breach these devices. As a result, the culture of information risks' awareness must be made available to people because these risks will not stay away. Thus, successful banks must adopt strategies to reduce those risks while providing effective solutions to their customers. In addition, there are legislations that ensure the privacy of individuals and address the misuse of the Internet, such as hacking and impersonation. Furthermore, there are positive aspects for using technology in banks such as reduction of workers' number, the rapid completion of transactions, reduction of costs, establishment of integrated systems, and improvement of decision making processes (Hanafi and Abu Kahf, 2004). Other positives aspects of modern technology in our contemporary world are demonstrated in China where a large number of Chinese use their mobile phones to pay a taxi fare, tuition fees, or to buy vegetables in simple amounts of money to such an extent that China, the country that invented the paper currency, could become the first one to abandon it. In large cities, payments made through mobile phones have dramatically increased. During the past year only, the value of purchases using phones had reached 5 billion dollars which indicates the durability of electronic commerce. Consumers were gradually moving away from traditional selling points as they prefer orders that do require only a few clicks from home or office to order food or to buy a ticket. Accordingly, China may become one of the countries that abandon cash currencies. On the other hand, older people are still reluctant to use smart-phones, and some old sellers say that the use of banknotes is easier as the they usually suffer from poor eyesight due to their old age, but sometimes they have to accept electronic payments because their customers do not have paper money (Economic, 2017).

In the Seychelles, Progress Soft Mobile Pay System (PS- M Pay) is utilizing smart-phone networks to offer a national service at the state level including all types of payments via smart-phones such as payments and transfers of funds among people (Person to Person) (P2P) or between people and institutions (P2B). The system also covers the means of payment from citizens to governmental institutions (Person to Government) (P2G), from companies to persons (Business to Person) (B2P), and from government institutions to persons (Government to Person) (G2P) regardless of the service provider of the user's smart-phone (The Middle East, 2012).

*1.3 Risks and Disadvantages of Using Information Technology on Electronic Banks*

1. Negative Impact on Bank's Reputation: Reputation risks arise in the case of negative public opinion towards the bank, which may extend to influence other banks, as a result of bank's inability to efficiently manage its systems or having them breached (Al Ganbehy and Al Ganbehy, 2006).
2. Negative Impact on Electronic Banking Transactions: The fast growth in e-banking transaction has created new challenges for banks and regulators as the management and bank staff may lack the adequate experience to cope with the rapid development of communication technology, as well as the increased fraud rate on the open networks such as the Internet, due to the absence of traditional practices by which the costumers' identity and legitimacy were ascertained. Therefore, the Basel Committee on Banking Supervision (BCBS) pointed to the importance of setting policies and procedures that allow the management of e-banking risks through their evaluation, supervision and follow-up (Badran, 2005).
3. Negative Impact on Bank's Strategy: the rapid developments in technology and the increasing rivalry between banks and nonfinancial institutions may expose banks to significant risks in case of adopting inadequate and insecure planning and implementation procedures for the strategy of electronic banking transactions. Accordingly, the bank management needs to carefully examine the contribution of the Internet strategy to maintaining the competitiveness and profitability of the enterprise.
4. Operating Disadvantages: The electronic open distribution channels leave banks with issues and challenges pertaining to secrecy and integration of information, and confirmations of customers' identity and legitimacy for bank accounts.
5. Legal Disadvantages: Banks are exposed to legal risks that may lead to the loss of some of their assets or to increasing their commitments towards others, due to the lack of a proper legal opinion or the inadequacy of legal documents as well as processing new types of transactions with the absence of a law that regulates such transactions. In addition, in some cases a new legislation is issued that affects the credit donor's claim of his full right in due date (Bekhtiar, 2010). The most highlighted legal challenge is represented in the situation of accepting the electronic contracts by the laws (Alzabin, 2012), in tax challenges, in the risks of high-tech crime, in the responsibility for errors and risks, and in the authenticity of electronic communication.
6. Money Laundering: the more the means of money laundering develop, the newer the techniques are evolved as a result of the huge technological advances, especially overseas

electronic transnational banking operations and transactions, such as opening bank accounts using the Internet, as well as transactions and other electronic banking operations that can be directly processed on-line.

*1.4 Information Hacking*

1.4.1 Internal Hacking

Internal hacking is often committed by individuals working within the bank. Those workers are able to hack confidential information more easily than external individuals. In this case, banks always solve the problem confidentially in order for businessmen not to lose confidence in the bank and not to harm the bank 's reputation.

The main reason for information hacking might be ascribed to financial gains, such as commercial tenders, and financial capacity of these projects, or to personal revenge, where some employers retaliate on the bank by hacking information and disclose it to others. Furthermore, the internal hacker can provide others with access points and electronic pathways to hack and access the organization’s confidential information.

1.4.2 External Hacking

External hackers are individuals who hack information security and access the banks’ secrets to steal the valuable information such as the banks’ financial secrets, franchise rights, futuristic plans for small businesses and banks and spying on others. Especially in the recent years, espionage operations have spread not only among countries, but also among financial and industrial companies; such as spying on inventions and scientific research carried out by these projects, whether large or small ones. Considering that hacking networks externally is not an easy task, hackers rely on human elements. They attempt to place one of their agents in the institution’s building, or to tempt and recruit one of the employees who work for the institution they want to hack. This method has proven its usefulness in many cases to the extent that it made internal hack more damaging to the institution than the external hack. For example, a bank manager leaves his office after a long day of work, leaving behind his documents and statements piled and exposed on his desk. Then, the cleaners, or the ones who impersonates them, enter the office to photocopy these documents and may find the manager’s password written on a sticky note paper on the screen of his computer. Such a case is considered a priceless hunt (Shabib, 2004).

1.4.3 Sabotage

Sabotage is to hinder the functions of computer system through disabling the intranet. Large organizations, universities, certain sovereign ministries such finance, banks, and small enterprises may utilize two types of networks; intranet and extranet. The intranet contains the organization’s sensitive and highly confidential information, while the extranet contains advertising information and is usually connected to the Internet. Usually, intra and extra nets are separate. The internal hacker can connect the two networks using a bridge or disable them by using viruses to enable the external hacker to access the internal network.

*1.5 Types of Hacking*

1.5.1 Impersonation

Impersonation is carried out by using Personal Identification Number (PIN) of some Internet users. The risk of impersonation occurs when the attacker steals the secret encryption key or captures the password during passing through the network and resending it later. Also, the attacker may change the message routing from the bank headquarter to one of its branches (Dawood, 2004). Many banks adopt the idea of entering the PINs using the mouse so as to prevent the attacker from capturing the PIN. Spying on the Internet and information networks in order to obtain a credit card number has become one of the problems that often costs the banks and insurance companies huge amount of money.

**Viruses** are named after human viruses that infect humans and animals alike because their attributes and characteristics are similar. These attributes include rapid spread, exactly like, epidemic diseases that spread among people as a result of a virus transmission from a person to another by infection, and that infect human body and damage it. Viruses have two main attributes.

**The First Attribute:** It is the disguise and the control over the infected program. The moment the infected program runs, viruses begin to work together immediately.

**The Second Attribute:** Computer viruses' transmission is similar to biological ones, where viruses reside in a key location in the computer such as Memory (RAM), and infect any file that is running. The more time spent in discovering the virus, the more difficult the virus destruction becomes (Zuhairi, 2010). A virus is a program or a set of instructions that causes damage to the information system or data. The virus has the ability to multiply and spread (Dawood, 2004).

*1.6 The Necessary Basic Elements to Protect Information*

- Secrecy: It means making sure that only the authorized people can access the information.
- Safety of Content: It is to make sure that the content of the information was not manipulated at any stage during processing.
- Continuity of Information Availability: It is to ensure the continuity of system's readiness and its ability to process data and information.
- Person Carrying an Information Related Act Denial Prevention: It means ensuring that the Person, who does an information related act, cannot deny what he committed (Makkawy, 2004).

*1.7 The Most Effective Means to Reduce Digital or Informational Crimes*

Specialists in information systems have several terms for the crimes that take place through using modern technology. While some specialists call these crimes financial embezzlement, others call them informational fraud and the others call them informational deception. All these terms are associated with the adaptation of modern technology in illegal and criminal thefts. Informatics is a two-syllable term, the first syllable is *Information* and the other one is

*Automatique*. In 1962, Drefus was the first to use the term informatics to distinguish the automated processing of information. Later in April 1966, the French Academy confirmed the term and defined it as "the science of logic processing of information" (Al-Shawa, 1994, p.20). Tredmann believes that informational crime includes any organized crime associated with the automated processing of information (Momeni, 2008). In the computer-related crimes report, the European council stated that the crime includes changing, erasing or writing data or computer software in addition to any other intervention in data processing in order to cause economic damage, or property loss or obtaining illegal economic gain for oneself or for others (Al-Saeed,1993). The principle of limiting digital crimes has attracted the attention of most countries in general and industrial ones, in particular, especially highly technical progressed countries that prosecute individuals for using computers to sell personal or governmental information or to modify software intending to cause harm to others. It is intended here that using traditional means such as theft, robbery or using modern technology such as the Internet in transferring funds between accounts is considered a theft. Due to over reliance on the Internet, the digital crimes increased, which led the governments in the Arab Gulf Council States to enact a series of judicial legislations to protect the Internet users. These laws have focused on several elements; legislations for customers and users of the Internet banking networks, in addition to legislations related to credit issues. Considering that the Internet is easy to access from anywhere, thus, legislations related to digital crimes should be applied in all countries around the world and not only to the country in which the crime has occurred and new integrated international legislation should be enacted. The main difficulty facing the international cooperation against informational crimes lies in the absence of common and mutual concept among countries in terms of the types of these crimes, and in lack of police and judiciary's expertise in investigating and collecting evidences for convicting criminals properly (Hitti, 2006)

*1.8 Some Means of Reducing the Digital Crimes*

1. Reducing the authorities to the lowest level; as a result, high privileges are associated with the higher levels of management only, and giving the authority of read-only access to users with the middle and supervisory levels, while continuing monitoring them.
2. Intensifying international cooperation all over the world to reduce informatics crimes.
3. Relying on advanced technical means such as using biometrics; fingerprints, eye and face scans.
4. Enacting laws that punish such crimes, whether committed in homeland or in a foreign country.
5. Upgrading the capacity of judges as well as employing experienced consultants.
6. Performing periodical audit and review operations for the protection and safety procedures.
7. Using firewalls with strong passwords, fingerprints and eye scanners.
8. Improving maintenance and infrastructure level.
9. Focusing on information security agreement concerning information crimes such as:

- fraud and forgery.
- Using pornography.

- Violating copyright.
- Financial and personal hacks.

## 2. Literature Review

Hani (2013) in her study titled "The Impact of Information and Communication Technology on the Algerian commercial banking activities" aimed to reveal the impact of information and communication technologies on the Algerian commercial banking activities by highlighting the reality of using technology by the Algerian banks and its application on the banks' various activities. The study was conducted on three banks in the city of Constantine. After testing the study hypotheses, the researcher concluded that the information and communication technology has a prominent impact on activating Algerian commercial banks' activities, but the latter have not been fully benefited from technology, as these banks are still at the beginning phase of taking advantage of information and communication technology. The study also concluded that the rest of modern banking services are not actually available because of several different reasons. Due to the effect of digital crimes on the efficiency of banks and as a result of high costs resulting from the financial losses caused by hacking data, the interest in knowing the most important sources of hacking and implementing successful strategies to fight against them has significantly increased. Some studies showed that there is a relationship between the digital crimes and the employee and client's social, financial, and cultural backgrounds. Studies also concluded that the physical work environment, career growth, responsibilities, positive relationships, commitment to systems, and efficiency of communication are the most effective factors in the digital crimes.

Haj (2014) in his study entitled as "Risks of Electronic Banking Operations" focused on the different risks that have a negative impact on banks and banks' customers including online fraud and forgery, and risk of operating; as many banks rely on a third-party handler to manage the appropriate technical infrastructure to support the banks' operations. Another source of operational risks is the protection; since the open electronic distribution channels raise important issues such as; the confidentiality and integrity of information, confirmation of customers' identity and legitimacy, and the control over customers' legitimate access to their accounts, especially with the increase in online fraud and forgery cases. In addition, credit risks are represented in the growing trend towards globalization in recent years, which has led to an increase in financial crises. Furthermore, some countries were affected by the economic crises of other countries. Most of the economic studies showed that the crises of banks have been the common denominator in the most financial crises, whether in developing or developed countries. Risks resulted from credit in addition to the mismanagement are the most important reasons for banks' stumbling and crises occurrence (Abdel-Kader, 2013). Banks must pay attention to the availability of external service providers and to the adequacy of their contracts. These contracts should be stated clearly and focus on the confidentiality and accuracy regarding collecting and using customers' information. In addition, regulatory authorities around the world should develop specific and sophisticated trends related to the allocation of technology. Rabah (2012) in his study titled "The Role of Banking Technology in Modernizing Algerian Banking System" highlighted the role of technical electronic banking services in developing and modernizing Algerian banks. The most prominent

conclusions are as follows:

- The Algerian banks suffer from a shortage in electronic banking services which are limited to using debt cards; despite the unused huge number of software programs.
- Creating a banking entity that is able to compete in light of financial and banking globalization is done only by adopting deliberate and appropriate strategies that take into account modern technologies in management.
- If Algerian banks enter the electronic world without an integrated strategy, a clear vision and appropriate modern technologies, they will fail because integration into the electronic economy requires huge investments in all areas and developments in protection and security means in order to ensure the confidentiality of all banking operations.

Yedo (2007) in his study titled "Information and Communication Technology (ICT) and Its Role in Modernizing" highlighted the effects of information technology on the banking system. The study concluded the following:

- The Internet and networks play a major role in the spread of e-commerce through the various services offered by all parties. Its importance relies on reducing costs, providing new opportunities, changing banking operations.
- Banks' adoption of modern trends in banking services increases the banks competitiveness, reduces the cost of providing services, and enables access to global markets.
- Accreditation of banks requires the existence of an infrastructure for information technology, which in turn contributes to the modernization of the Algerian banking system and gives it a competitive ability to cope with global developments.
- In Algeria, the stumble in updating payment methods is ascribed to a number of obstacles such as the legislations of electronic payment and e-commerce, and the high cost of setting-up and maintaining electronic banking networks.

Ahmad (2010) in his study entitled as "The Impact of Modern Technology on Banking Services in Sudan" revealed that the banking technology leads to an increase in bank deposits and profits and in the amount of work done and a decrease in costs. The most important drawbacks of using modern technologies are continuous power cuts, and breakdowns of communications networks. It is of utmost importance to strengthen efforts to spread the culture of digital and information society. Al-Akabi et al. (2008) in their study entitled as "Electronic Money and Its Role in Fulfilling Contractual Obligations: Safety and Confidentiality" stated that the most important features of electronic money are security and confidentiality. Security means that the process of electronic money transfer is made in a way that no one can modify it. Confidentiality means the electronic transaction is made anonymously and no one can have access to the electronic payment systems, due to the advanced technology of cards and modern programs that initiate a secure secret electronic communication between e-cash users (Matonis, 1995). However, the issue is not that easy as electronic dealing is fraught with security and hacking risks, which can be done by tracking the owner of the electronic money while making the deal. The most notable examples are the

theft of financial information and contracts, and disabling the web sites by hackers (Goldfinger & Herbin, 1999). In fact, the security breach of electronic transactions is manifested in software based money which is connected to the Internet.

Naji (2004) in his paper titled "Towards a Practical Program for Developing the Security Role of Educational Institutions" highlighted the university role in preparing studies and research projects and in focusing on intellectual security for next generations. The paper assured the university mission in applying knowledge and scientific research in informatics security (Naji, 2004). The paper has focused on the awareness and intellectual security culture as a cornerstone in fighting information crimes. Husseini (2008) in his study titled "Information Security for Information Systems" explained the importance of information security as an equally important element to other production elements such as capitals and individuals (Husseini, 2008). The study focused on security tools and modern technical means and software such as surveillances cameras, secret codes, magnetized cards, fingerprints and eye scanners which protect information from hackers. The study also assured the necessity of providing specialized equipment and cadres for maintaining the security and efficacy of information. Nasseef (2009) in his study titled "The Management Information Systems and Their Role in Improving the Quality of Banking Services" mentioned the dimensions of service quality as a prerequisite and identified ten criteria for evaluating the quality of services using the model of Rayport and Sviokla that was introduced in 1994 as presented in the following table (1):

Table 1. Dimensions of Measuring the Quality of Services

| Dimension | Definition |
|---|---|
| Credibility | Being trustworthy and reliable (the possibility of placing confidence in the service), and honesty and straightness of the provider. |
| Security | Free from risks resulting from using the electronic banking services. |
| Ease of Accessing the Service | Accessing the service easily. |
| Telecommunications | Listening to customers and guiding them using the language they understand. |
| Understanding Customers | Setting efforts to understand and fully identifying customers' needs. |
| Tangibility | Showing the physical facilities, equipment, people, and means of communications. |
| Reliability | The ability to accomplish promises of service accurately and truly. |
| Response | Management prompt response to help small business clients and provide them with immediate service. |
| Efficiency | Possessing the required skills and knowledge. |
| Courtesy (Civility) | Respect, consideration of others feelings, friendship with contacts, and being friendly. |

These ten dimensions have been incorporated into five dimensions; reliability, response, trust, empathy, and physical tangibility (Alavichat, 2001). These five dimensions will be clarified to illustrate the extent of the customer's understanding of them:

- Reliability: It is defined as the ability to deliver service reliably (delivery on time), and to accomplish the service accurately which means trustworthy.
- Response: It represents the customers' awareness of getting their problems solved promptly and accessing the services quickly, continuously and on-demand.
- Affirmation and confidence: It is a very important dimension in banking business, as some bank employees are required to be consulted on high risk operations such as financial and in-kind investments. In addition, the bank's role in insuring investment risks and in gaining customers' confidence is provided as a result of previous experiences with the clients.
- Empathy: It means dealing with customers personally and individually on the basis that the customer is a unique person who should be given a special treatment and care.
- Physical tangibility: It includes building's exterior outlook, modern technologies, and employee's appearance. Banks focus on the physical tangibility to improve their image in customers' eyes such as the shape of the external and internal parts of the building, and advanced technologies implemented to give the customers an image that their bank is offering superior services than other banks (Nasseef, 2009).

Thus, the previous studies have shown that the negative aspects of using technology in banks have become uncontrolled complicated challenge. This research concluded that it is necessary for electronic money to undergo a special and appropriate legislation, especially since the country is witnessing a new legal openness and is in an urgent need to develop its legal and economic systems. These systems should contain clear and precise legal rules to maintain peoples' funds and the interests from manipulation or theft. It should also include restrictions and controls for institutions entrusted with issuing electronic money as these institutions must be under direct supervision of the Central Bank. Furthermore, credit institutions should introduce the new telecommunications technology and they should be encouraged to establish economic relations and banking transactions with institutions all over the world in order to be updated with the latest developments in the field.

### *2.1 Commentary on Previous Studies*

The previous presentation of studies and research on electronic banking shows that a number of studies focused on the social and educational backgrounds and their role in fighting against hacking confidentiality of information, while other studies focused on the role of commercial banks in combating this phenomenon using their managerial and technical capabilities. Moreover, other studies focused on the legal view of controlling information hacking and manipulation. Finally, the rest of the studies focused on the state's ability in providing the appropriate infrastructure.

The present study focuses on the negatives of information hack on commercial enterprises clients and on the banks' role in fighting such hacking, implementing futuristic necessary strategies, and in revealing the threats facing the banking industry such as hacking operations

to accounts, statements, and transactions which may lead to the loss of confidence in these banks.

## 3. Methodology

This part of the study tackles the design of the study instruments and its procedures. It also covers the participants, the instruments and the duration of the experiment. Due to the nature of the enquire, the author decided to best follow a quantitatively based design. The quantitative design of the study utilized a questionnaire as the primary data collection instrument. A questionnaire was administered to participants who were asked to complete it. Data was collected, and then tabulated, and processed using the statistical package for social science (IBM SPSS Statistics®) version 22.

### *3.1 Participants*

A group of 300 (240 male and 60 females – see Figure 1) Saudi banks' customers and small entrepreneurs were randomly selected to explore the positive and negative impacts of using electronic banking in their opinion. Participants were of different age ranges (See Figure 2).

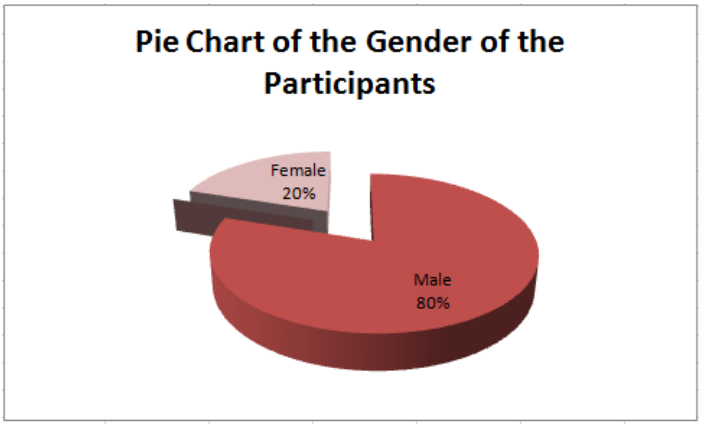


Figure 1. Pie Chart of the Gender of the Participants.

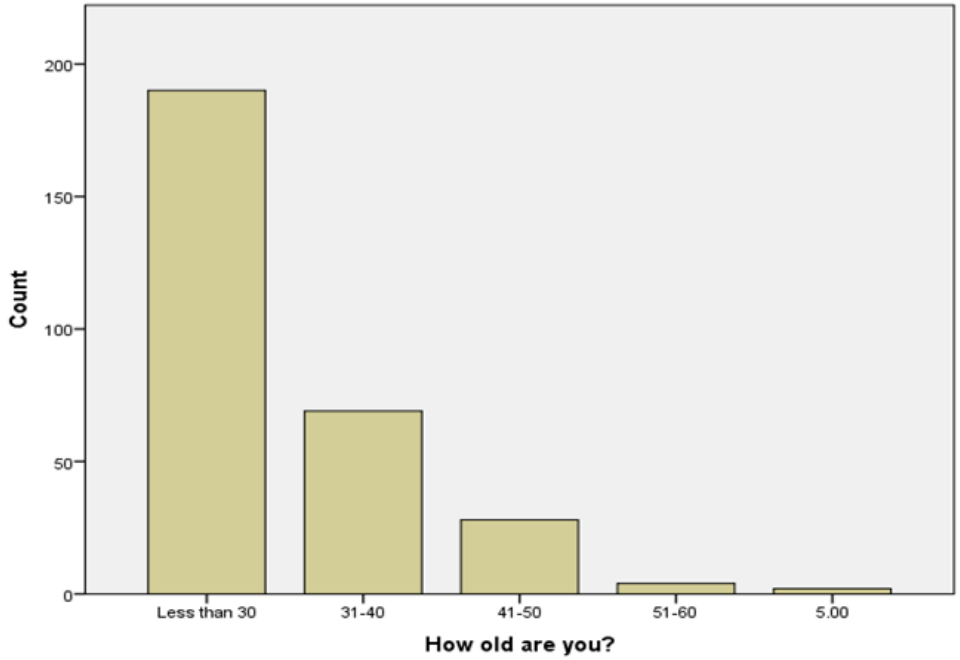


Figure 2. Bar Chart of the Ages of the Participants.

As can be seen in figure 2, the majority of the participants were younger than 30 years old (190participants - 64% of the total number) whereas the least number of participants were 51-60 years old (4 participants - 1% of the total number). Furthermore, there were 240 male participants and 60 females.

The study covered the majority of the Saudi banks and their services in the Western region of the Kingdom of Saudi Arabia. Participants were informed about the study purpose and their approval to participate in the current study was recorded.

*3.2 Study Instruments*

In order to achieve the study objectives and aims, a questionnaire was used as a tool to collect the primary data. The questionnaire consisted of forty-four (44) items on a five (5) point Likert scale to elicit participants' responses, which were confidentially treated. Responses were coded for the purposes of analysis in IBM SPSS Statistics 22®.

3.2.1 Validity of the Questionnaire

***a. Face validity of the questionnaire***

The researcher used the content validity to validate the questionnaire. The questionnaire was introduced to a group of specialists in order to:

a) Determine the suitability of the suggested items to participants.
b) Add, omit or modify other components.

Hence, the study questionnaire was constructed on the bases of the specific objectives. The questionnaire was submitted to a panel of qualified and experienced specialists. They were requested to evaluate the linguistic features of the items, appropriateness and fitness of the

items for the participants, applicability for the participants, and how the items measure the study objectives. Their suggestions were taken into consideration. They confirmed the suitability and applicability of the questionnaire.

***b. Internal Consistency***

The validity of the questionnaire was determined by internal consistency. The internal consistency for each item in the questionnaire was calculated by using (Pearson Correlation) formula. Table (2) shows the internal consistency of the questionnaire items.

Table 2. Internal consistency of questionnaire items

| Internal Consistency of the questionnaire items | Internal Consistency |
|---|---|
| Item 1 | 0.893 |
| Item 2 | 0.923 |
| Item 3 | 0.898 |
| Item 4 | 0.725 |
| Item 5 | 0.765 |
| Item 6 | 0.768 |
| Item 7 | 0.817 |
| Item 8 | 0.731 |
| Item 9 | 0.812 |
| Item 10 | 0.793 |
| Item 11 | 0.869 |
| Item 12 | 0.805 |
| Item 13 | 0.845 |
| Item 14 | 0.810 |
| Item 15 | 0.700 |
| Item 16 | 0.808 |
| Item 17 | 0.764 |
| Item 18 | 0.826 |
| Item 19 | 0.810 |
| Item 20 | 0.848 |
| Item 21 | 0.740 |
| Item 22 | 0.741 |
| Item 23 | 0.746 |
| Item 24 | 0.720 |
| Item 25 | 0.861 |
| Item 26 | 0.804 |
| Item 27 | 0.816 |
| Item 28 | 0.704 |
| Item 29 | 0.821 |
| Item 30 | 0.728 |
| Item 31 | 0.845 |

| | |
|---|---|
| Item 32 | 0.707 |
| Item 33 | 0.858 |
| Item 34 | 0.836 |
| Item 35 | 0.839 |
| Item 36 | 0.734 |
| Item 37 | 0.715 |
| Item 38 | 0.878 |
| Item 39 | 0.869 |
| Item 40 | 0.854 |
| Item 41 | 0.870 |
| Item 42 | 0.816 |
| Item 43 | 0.708 |
| Item 44 | 0.851 |

3.2.2 Reliability of the Questionnaire

The questionnaire was administered to the participants. The data obtained was computed to calculate the reliability coefficient. It resulted in a value of 0.925**. The reliability coefficient of the questionnaire scores was determined by split half method. According to McQueen and Knussen (1999), split half reliability is the simplest and most direct method for demonstrating reliability. Gronlund (1990) reported that the reliability coefficient typically ranges between (0.60-0.80). Aiken (1985) and Warner (2012) assured that a questionnaire should have a reliability coefficient ranging from 0.7 and preferably closer to 0.9 to be considered useful. Thus, the reliability coefficient of this questionnaire is considered within the acceptable range. In addition, Cronbach's Alpha coefficient (α) was calculated to ensure the internal consistency of the questionnaire. Cronbach's Alpha coefficient was calculated at 0.905 for the questionnaire and this value ensured that the test is valid and reliable as shown in the following table:

Table 3. Cronbach's Alpha coefficient

| **Alpha Cronbach' s values (Cronbach' s alpha)** | **Internal consistency** |
|---|---|
| $\alpha \geq .9$ | Excellent |
| $.9 > \alpha \geq .8$ | Good |
| $.8 > \alpha \geq .7$ | Acceptable |
| $.7 > \alpha \geq .6$ | Questionable |
| $.6 > \alpha \geq .5$ | Poor |

*3.3 Data Analysis of the Constructs*

Certain items analysis will be presented in this section. According to the responses collected from the participants to the survey, the majority of the participants expressed concerns about their personal information and at the same time, they majority of the participants expressed their support towards technology and utilizing it in the e-banking systems. The first eight items in the questionnaire dealt with the issue of customer personal information and the risk of having it compromised. The following table, Table 4. Shows the responses of the

participants to the first eight items.

Table 4. Participants' responses to the first eight items relating to customer sensitive information

| Item | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| Disclosure of customer information such as name, address, account number and telephone numbers contributes to embezzlement. | 162 | 84 | 21 | 24 | 9 |
| Customer's indifference to the importance of confidentiality, such as giving the pin number to relatives or anyone in case of asking for help to use the ATM machine. | 135 | 104 | 22 | 21 | 18 |
| Giving a bank employee the freedom to deal with the client's assets such as buying and selling shares contributed to embezzlement | 122 | 111 | 29 | 23 | 15 |
| The ability of external hacker to disrupt computer systems in bank | 86 | 109 | 67 | 32 | 6 |
| The inability of customers to use modern technology, leads to financial losses for them | 68 | 105 | 68 | 54 | 5 |
| Credit cards are always misappropriated | 46 | 110 | 90 | 51 | 3 |
| Most bank break ups are internal penetrations | 27 | 87 | 130 | 48 | 8 |
| The external hacker can view customers' accounts | 54 | 127 | 66 | 44 | 9 |

As can be seen from the above table, the majority of the customers expressed their agreement regarding concerns of personal and sensitive information which might be compromised if mishandled by the banks. With regards to the participants opinion on the use of electronic banking and if they believed the use of modern and advanced protecting electronic systems will lead to minimizing such risks, the following table, Table 5. highlights the responses of the participants.

Table 5. Responses to items 9, 10 and 11 (Electronic Banking/Money vs. Conventional Banking/Money)

| Item | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| Electronic banks will replace traditional banks in future | 58 | 103 | 57 | 50 | 32 |
| Using the modern systems by bank, contributes to minimizing the external and internal hacking | 136 | 104 | 40 | 20 | 0 |
| Electronic money will replace conventional money | 62 | 79 | 61 | 62 | 36 |

As the above table shows the majority of the participants agreed to statements that electronic banking/money will replace conventional banking and money. Over 50% believed that

electronic banks will replace conventional banks. Over 80% believed that if banks used advanced electronic protecting systems, they will minimize external as well as internal hacking. With regards to the statement that electronic money will replace conventional money, almost 50% believed that it will, 20% were undecided and 30% believed it will not.

With regards to items 12, 13, 27, 28 and 32 in the questionnaire which are related to the laws and legislations that governments around the world have set in place to combat electronic crimes, the responses are presented in the following table (Table 6).

Table 6. Responses to items 12, 13, 27, 28 and 32

| **Item** | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| Judicial laws are somewhat imprecise | 60 | 77 | 76 | 73 | 15 |
| Criminal laws didn't develop to accommodate new types of computer crimes | 71 | 100 | 75 | 51 | 3 |
| Judicial laws are not strict enough to protect personal information online. | 60 | 78 | 92 | 51 | 14 |
| Judicial laws lack the suitability and proportionality in keeping up with modern technological and legal issues in e-Banks | 63 | 102 | 72 | 43 | 18 |
| The existence of international banks necessitates the devising of a unified anti-online crime laws so as to prevent money embezzlement | 116 | 105 | 69 | 8 | 2 |

As can be seen from table 6 above, the majority of the participants agreed that judicial laws are imprecise, need updating, need to be strict enough and governments around the world need to be having a unified set of judicial laws in order to protect the public from hacking and electronic thefts. It was interesting to see that many of the participants were undecided and that could be attributed to the lack of knowledge of these issues amongst those participants.

The largest proportion of the questionnaire related to the risks of hacking and the vulnerability of bank customers online when their information is compromised due to hacking, failure of the system due to computer viruses or even due to few dishonest bank employees who may themselves commit money thefts. The latter issues are represented in items 18, 19, 20, 21, 22, 23, 24, 25 and 26. Table 7 highlights the responses of the participants to these issues.

Table 7. Responses to items 18, 19, 20, 21, 22, 23, 24, 25 and 26

| **Item** | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| There are some risks that accompany using the ATM machines as the disclosure of the PIN number | 72 | 159 | 38 | 30 | 1 |
| The internal hacker can view customer's balances | 104 | 121 | 42 | 22 | 11 |

| | | | | | |
|---|---|---|---|---|---|
| and personal secrets | | | | | |
| There is a breach of information in electronic banks | 65 | 104 | 71 | 44 | 16 |
| Most of the penetration of e-banks are externals | 57 | 93 | 82 | 53 | 15 |
| Most money thefts/ traditional theft are done during ATM withdrawal | 72 | 126 | 68 | 31 | 3 |
| The increase of virus attacks on e-banking websites damage these banks | 130 | 98 | 43 | 19 | 10 |
| Most e-pay methods susceptible to embezzlement are credit cards | 112 | 133 | 46 | 7 | 2 |
| There is a relationship between embezzlement of bank customers and some corrupted bank employees | 73 | 83 | 97 | 41 | 6 |
| External hacking is made via the help of some corrupted bank employees | 40 | 79 | 109 | 54 | 18 |

Table 7 above illustrates that the majority of the participants shared the agreement on the concerns about credit card frauds, susceptibility to embezzlement as well as risk of external and internal hacking. It is clear that most participant believed that there is a serious risk when the PIN number of the ATM card is compromised (77%) as well as the risks of fraud from credit card thefts (82%). Similarly, they believed that attacks on banks' websites are quite serious (76%) as well as the risks when an internal hacking occurs leading to the customer's balance being stolen (75%). To a much lesser extent and only slightly, a large proportion had negative views on banks and internal hacking via few corrupted bank employees. This is evident in large number of "undecided" responses from the participants.

### *3.4. Study Delimitation*

The present study is limited to the following factors:

1- The study is limited to the Saudi context.
2- Participants' awareness of the provided e-banking services was noticeably limited.

## 4. Conclusions

1. The inability of many Arab countries' legislations to keep up with the recent developments, affects the banks' ability to continue in light of the fierce global competition in the banking sector which affects on customers' and small entrepreneurs' confidence towards the laws that govern electronic transactions and their ability to protect them from financial risks while dealing with banks.
2. The willingness of the banks in such countries to take advantage of the technological developments to provide better services for their customers made them sign contracts determining rights and obligations, and ensuring themselves huge privileges at the expense of their clients, taking advantage of the legislative vacuum in this field.

## 5. Recommendations

For the security of electronic banking, banks and their management should take into account the following requirements (Safar, 2006):

1. Banks should take the proper procedure in regard of identifying and separating responsibilities, duties, databases and applications.
2. Banks should take appropriate measures to protect the confidentiality of information.
3. Assigning responsibilities for electronic banking systems users.
4. Sensitive and high-risk data should be stored on computer systems to be recovered and matched.
5. Employing specialized judicial entities in electronic banking issues.
6. There should be official entities that spread confidence among investors.

Obliging banks to financially compensate customers in the case of hacking their accounts and withdrawing huge sums of money by insuring their assets and shares. The insurance should be proportionally matched with the financial amounts of money.

## References

Abdel-Kader, R. (2013). Banking risk management in accordance with Basel decisions 2 and 3 and the requirements of achieving the global financial and banking stability after the global financial crisis. Social Science journal, University of Mohamed KHIDER, Biskra, 29, p. 27.

Ahmad, H. (2010). Impact of modern technology on banking in Sudan. Sudan University of Science and Technology, Sudan.

Aiken, L. R. (1985). Three Coefficients for Analyzing the Reliability, and Validity of Ratings. *Educational and Psychological Measurement, 45,* 131-142. https://doi.org/10.1177/0013164485451012

Al-Akabi, B., et al. (2008). Electronic money and its role in fulfilling contractual obligations. Journal of Ahl al-Bayt, 6th ed.

Alavichat, T. (2001). The impact of quality and customer satisfaction in determining marketing strategy for banking service, an analytical study on a sample of Jordanian commercial banks. Ph D thesis, College of Management and Economics, University of Mosul, Iraq.

Al-Fateh, H. M. et al., (2011). Communication and Modern Media Technology; Usage and Effect. Knoz Alhekma for publishing and distribution, Algeria, p. 2.

Al Ganbahy, M., & Al Ganbahy, M. (2006). Electronic Banking. University Thought House, p.231.

Al-Saeed, K. (1993). Computer crimes and other crimes in the field of information technology. working paper submitted to the Sixth Conference of the Egyptian Society for Criminal Law, Cairo, Dar Al Nahda.

Al-Shawa, S. (1994). Information revolution and its impact on the Penal Code. Cairo, Arab Renaissance Publishing House, p. 4.

Al-Zabin, S. (2012). Electronic funds transfer and the legal responsibility of banks. 1st ed, Culture House for Publishing and Distribution, Egypt, p.212

Badran, A. (2005). Modern management of banking risks under the Basel 2. *Accredited Accountant, 3*(23), 12.

Bakhtiar, H. (2010). The bank responsibility in documental accreditation and risks. 1st Edition, Legal Books House, Shatat software publishing House, Egypt, pp. 317

Dawood, H. (2004). The security of information networks. Institute of Public Administration, Riyadh.

Economic Newspaper. (2017). Growing Interest for Electronic Transactions in Place of Cash Currency in China. 23rd of July 2017.

Goldfinger, C., & Herbin, P. (1999). How to Regulate Issuers of E-money? Issue Paper prepared on behalf of IPTS.

Gronlund, E. N. (1990). Measurement and Evaluation in Teaching.

Haj, H. (2014). Risks of electronic banking operations. University of Ouargla, Algeria.

Hanafi, A. G., & Abo Kahf, A. S. (2004). Modern Management in Commercial Banks. University House, Alexandria, p. 375

Hani, M. (2013). The Impact of Information and Communication Technology on Algerian commercial banks' activities. University of Ouargla, Algeria.

Hitti, M. (2006). Computer Crimes. Oman, Curricula House for publication and distribution.

Husseini, S. (2008). Information security for information systems. unpublished Master thesis, Baghdad. Retrieved from http://www.iraqstudent.net/detail.php?recordID=694

Makkawy, M. (2004). The digital environment between cons of reality and the hopes of the future. Cybrarians Journal.

Matonis, J. (1995). Digital Cash and Monetary Freedom.

McQueen, R. A., & Knussen, C. (1999). Research Methods in Psychology: A Practical Introduction. Prentice Hall.

Momeni, N. (2008). Informatics Crime. Amman. House of Culture.

Naji, M. (2004). Towards a practical program for developing the role of educational institutions. working paper submitted to the symposium of community and security, King Fahd Security College, Riyadh.

Nasseef, O. (2009). Information Management systems and their role in improving the quality of banking services. University of Al-Andalus magazine, Sana'a, Yemen.

Rabah, A. (2012). The Role of Electronic Banking Technology in the Modernization Of Algerian Banking System, Academic Journal of social and human studies, Issue 8, pp12

Rayport, J. F., & Sviokla, J. J. (1994). Managing in the Market space, Harvard Business Review, pp 141-150.

Safar, A. (2006). Electronic Banking Business in Arab countries. Modern enterprise for the book, p. 226

Shabib, A. (2004). Protecting Information has become an issue of the protecting the national economy. Middle East newspaper, Issue 9292.

The Middle East Newspaper (2012). Payment services via mobile phone opens new economic prospects. Modernization of Algerian Banking System. Academic Journal of social and human studies, Issue 8, pp12.

Warner, R. M. (2012). Applied Statistics: From Bivariate Through Multivariate Techniques: From Bivariate Through Multivariate Techniques: SAGE Publications.

Wikipedia. (2015). Information security. Wikipedia, the Free Encyclopaedia. Retrieved May 2017.

Yedo, M. (2007). ICT and its Role in the Modernizing Banking Services. Master thesis, Saad Dahlab University, Blida, Algeria.

Zuhairi, T. (2010). Personal computer and information security requirements. Mustansiriyya University, Baghdad.

**Copyright Disclaimer**

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).