

## **CYBER CRIMES AND BUSINESS GROWTH - A STUDY OF ONLINE BANKING SECTORS IN BAHRAIN**

*Liaqat Ali*

AMA International University, The Kingdom of Bahrain

### **ABSTRACT**

Cyber crime is one of the most important issues to be considered when dealing with online banking services. Computer fraudsters are always trying to gain unauthorized access to the information of financial and business sectors for fraudulent activities. Security developers are applying several techniques to enhance security layers but computer fraudsters are always few steps forward. No doubt, the effects of cyber crimes are more than the financial integrity of financial institutions and other organizations. For appropriate measurements to be implemented, organizations must understand the effects of cyber crimes. Cyber crimes affect the business growth in the country where more security measures should be adopted for the purpose of secure online banking environment. The current research paper explores issues of online banking sectors in the Kingdom of Bahrain and provides suggestions on how to further enhance the security of these online banking sectors.

**JEL classification codes:** G20, H20, L80, M10, M15

**Key words:** Cyber Crimes, Online Banking, Security, Business, Bahrain

**Corresponding author's e-mail address:** [liaqat22@gmail.com](mailto:liaqat22@gmail.com), [l.ali@amaiu.edu.bh](mailto:l.ali@amaiu.edu.bh)

### **INTRODUCTION**

Illegal activities conducted by fraudsters and criminals using electronic means such as computers and other network devices are genus of crimes which are transitional in nature compare to traditional crimes. The rapid growth in cyber crimes is the main concern for financial institutions in 21st century and the need to protect the cyber space is becoming more critical than ever before.

The word 'Cyber Crime' covers a range of crimes that are conducted virtually using any source of internet. This includes sending or spreading virus programs, hacking and cracking, spam emails, phishing and obtaining unauthorized access to other computers to steal financial information.

Cyber crime is one of the burning issues in today's online banking industry in the world. No doubt, the effects of cyber crimes are more than the financial integrity of financial institutions and other organizations. For appropriate measurements to be implemented, organizations must understand the effects of cyber crimes. Financial organizations must be aware of online threats and must take into consideration all those measure that can help in improving the awareness of individuals in regard of security and to maintain sustainable financial business environment in The Kingdom of Bahrain industry.

In fact, 100% security can never be implemented to protect banking sectors from online threats as computer fraudulent and cyber criminals are always to be found two steps forward than security managers. The important element is to find that how the security of online banking could be improved and how the effects of these online threats could be minimized to maintain secure and sustainable business in financial organizations.

This research, therefore, covers issues relevant to online banking particularly in industry of the Kingdom of Bahrain.

### **RESEARCH BACKGROUND**

The rapid growth of Information Technology and mobile networks has led to the development of information society in the modern world. Although this development provides and facilitate computer users to collect information with their finger tips but there are issues that must be considered and security is one of them. Research proved that computer fraudsters have attempted to gain access many times against information infrastructure and other internet services to steal financial information of online banking customers and the financial damage resulted by these unauthorized access by the computer fraudsters and criminals resulted to be enormous.

Cybercrime and cyber security goes in parallel. Enhancing the layers of security and to protect information infrastructure is critical for security managers to maintain secure business environment particularly when dealing

with online banking services and other sensitive financial transactions. Somehow it is a shared responsibility as institutions and customers both are responsible to make sure that necessary considerations are in place but it is important that financial organizations must provide such tools that can provide online banking customer a secure access 24 hours a day and 365 days a year.

Online banking has been around since 1981, nearly no cases of fraud have been reported until 2004 (Sia Partners, 2013). After 2004, a rapid increase has been seen and many attempts were made by computer fraudsters and cyber criminals to gain unauthorized access to steal financial information of banking customers. The estimated annual cost over global cyber crime is 100 billion (GoGolf, 2013). In addition the current estimates value the Middle East cyber security sector at \$25 Billion over the next 10 years (Kirsty, 2015). Therefore, researchers are warning the Middle East is becoming the hot spot for the cyber crime and other online fraudulent activities by the cyber criminals. The Kingdom of Bahrain is therefore can never be ignored when handling issues such as cyber crimes.

The Kingdom of Bahrain certainly understands the sensitivity of cyber crime activities and therefore different legislations have been drafted to be implemented to provide secure environment when dealing with online banking and other financial sectors. In this case, the major Bahrain legislation associated to cyber crimes are currently the constitution, The Penal Code, The Telecommunications Law and the Central Bank of Bahrain Law of its regulatory framework. The Kingdom of Bahrain will also introduce a new law of cyber crimes once it is approved by the Shura Council (OxfordBusinessGroup, 2015).

According to the report presented by the Kaspersky Lab based on data from Kaspersky Security Network of 2014, it was found that Saudi Arabia was recorded the highest in terms of online fraudulent activities followed by UAE. However, Bahrain was reported to be the most secure country in Gulf region for cyber crime activities but again it is important to consider that malware detection was 17.7% recorded which shows that threat is still available to the economy due to cyber activities (Mishra, 2014).

The main Bahrain legislation relevant to cyber crime is currently the Constitution, the Penal Code, the Telecommunications Law, and the Central Bank of Bahrain Law and its regulatory framework.

The challenges facing to online security particularly online banking are global and could only be addresses if appropriate measures and strategies are in place by the government and other financial institutions. This needs a comprehensive approach to fight against cyber criminals and computer fraudsters by developing adequate legislations and appropriate legal framework to secure online financial transactions and other activities.

## **CASE OF ONLINE BANKING SECTORS IN THE KINGDOM OF BAHRAIN**

Cyber crimes are becoming increasingly sophisticated in the Kingdom of Bahrain's business industry and the government of Bahrain needs to warn business about cyber crime threats and other activities. The Central Bank of Bahrain is the main bank of The Kingdom of Bahrain and the website of the bank could be accessed on <http://www.cbb.gov.bh/>. According to database of Central Bank of Bahrain there are about 403 financial institutions registered in The Kingdom of Bahrain (CBB, 2016). These financial institutions are categorized as followings;

**TABLE 1 – TOTAL NUMBER OF BANKS IN THE KINGDOM OF BAHRAIN**

Conventional Banks / Retail	22
Conventional Banks / Wholesale	56
Islamic Banks / Retail	6
Islamic Banks / Wholesale	19
Insurance Licensees / Locally Incorporated Insurance Firms	25
Insurance Licensees / Overseas Insurance Firms	11
Insurance Licensees / Insurance Broker	31
Insurance Licensees / Insurance Managers	5
Insurance Licensees / Insurance Consultants	4
Insurance Licensees / Insurance Firms (Restricted to Business Outside Bahrain)	19
Insurance Licensees / Insurance Brokers (Restricted to Business Outside Bahrain)	4
Insurance Licensees / Insurance Consultants (Restricted to Business Outside Bahrain)	2
Insurance Licensees / Registered Actuaries	27
Insurance Licensees / Registered Loss adjusters	11
Insurance Licensees / Insurance Pools & Syndicates	2

Investment Business Firms / Category 1	20
Investment Business Firms / Category 2	13
Investment Business Firms / Category 3	18
Specialized Licenses / Money changers	19
Specialized Licenses / Fund Administrator License	3
Specialized Licenses / Registered Administrators	1
Specialized Licenses / Financing Companies	8
Specialized Licenses / Banking Representative Offices	9
Specialized Licenses / Insurance Representative Offices	4
Specialized Licenses / Investment Firm Representative Offices	8
Specialized Licenses / Microfinance Institutions	2
Specialized Licenses / Trust service providers	3
Specialized Licenses / Ancillary Service Providers	16
Specialized Licenses / Insurance Ancillary Services	6
Specialized Licenses / Societies	3
Specialized Licenses / Registered Professional Body	1
Capital Markets / Licensed Exchanges	2
Capital Markets / Licensed Clearing, Settlement and Central Depository Systems	1
Capital Markets / Licensed Securities Broker-Dealer	13
Capital Markets / Licensed Securities Clearing Member	6
Capital Markets / Licensed Securities Broker	4

## STATEMENT OF RESEARCH PROBLEM

Current security measurements in banking sectors require the use of appropriate applications to secure online banking and to minimize available threats in cyber space. However, there is disagreement on whether security can be provided with its maximum level or the battle between security managers and computer criminals will never be ended. The effects of cyber crimes on business growth can never be ignored and must be addressed to develop awareness among individuals particularly in banking and other financial sectors to maintain secure and sustainable financial business environment.

## AIMS AND OBJECTIVES

### Aim

The aim of this research is to analyze the factors of cyber crimes affecting the growth of banking sectors in The Kingdom of Bahrain's industry. The alternative aim of the research is to recommend and discuss that how security layers could be improved to maintain sustainable business growth in banking and other financial sectors.

### Objectives

The objectives of this research are followings;

- To critically analyse the role of online banking customers to reduce information security risks in banking sectors
- To critically review the role of information security tools to maintain the security of information system in banking sectors
- To critically analyse the effects of cyber crimes on The Kingdom of Bahrain banking sectors
- To recommend measures to improve the level of security of online banking applications and to maintain sustainable business in banking security in the Kingdom of Bahrain

## RESEARCH QUESTIONS

Following are the research questions to achieve above objectives of this research;

- What is the role of individuals/online banking customers to reduce the available risk of online threats when dealing with banking applications?
- What tools and other safeguard software/applications can help in minimizing the risk of cyber threats.

- What factors must be considered to improve the level of security and to develop awareness among online banking customers by the banking industry to maintain secure and sustainable business in banking sectors?

## **RESEARCH IMPORTANCE AND SCOPE**

The significance of this study can be measured by the effective outcomes of security recommendations made in this research to improve the layers of security and to manage secure online business in banking industry. The research will be beneficial for those financial organizations looking to develop awareness among individuals from security perspective and facilitate them with the recommendations that must be considered when dealing with online threats. The research is also beneficial for business administration students and other individual readers to develop concept about online banking services, its security and importance and to have a comprehensive idea about the issues relevant to cyber crimes and its effects on online banking services and other business sectors. The scope of the research could be measured through the scope of security and its implementation in online banking sectors of The Kingdom of Bahrain. The resources needed to complete this research were also very limited and therefore the author is feeling that there is need to conduct more comprehensive research when it comes to online businesses particularly in online banking sectors of The Kingdom of Bahrain.

## **RESEARCH NOVELTY**

The novelty of this research is based on the comprehensive approach adopted to understand the seriousness of The Kingdom of Bahrain business sectors in online banking industry. The research is not limited to any specific organization or financial institution and the author took extreme care and efforts to find the overall effects of cyber crimes and discusses issues on how to improve the security layers when dealing with online banking services and other electronic financial transactions. The research is unique due to the nature that it details effects of criminal cyber activities on business growth and recommend measures on how to maintain secure and sustainable electronic banking when dealing in cyber space. Furthermore, people from different disciplines of life actively participated in the survey of this research. It was found that all respondents showed high interest in the survey of this research and therefore made this research a unique research paper.

## **RESEARCH RATIONALE**

The research is taken due to the importance of security issues of online banking services. The author is interested in the study of security of cybercrimes and business studies and therefore conducted this research to find out and discuss factors of cybercrimes affecting the growth of business sectors in Bahrain particularly online banking services.

## **RESEARCH LIMITATIONS**

The current research provides comprehensive approach in understanding issues relevant to cyber crimes, its effects on business growth and online banking services but still limited due to many reasons. One of the important elements to be considered here is the timeframe of current research. The research is limited due to limited time available and therefore may not provide complete picture and recommendations when it comes to increase the security of online banking services. The research conducted a survey to understand the behaviour of banking customers when dealing with online applications and other transactions but is limited due to limited responses collected from different high street banks in The Kingdom of Bahrain. The difficulty in approaching to online banking customers, people do hesitate when discussing about their online banking, also made difficult to form this survey. This hesitation of online banking customers leads to increase the limitation of this research. The survey of this research is also limited to online banking customers and limited opinion was collected from the banking industry in Bahrain. Further, the research is limited to the discussion and case study of the following 8 high street banks in the Kingdom of Bahrain;

1. Ahli United Bank (AUB) ([http://www.ahliunited.com/bh\\_retail.html](http://www.ahliunited.com/bh_retail.html) )
2. Al-Salam Bank Bahrain (<http://www.alsalambahrain.com> )
3. Bahrain Islamic Bank (<http://bisb.com/> )
4. BBK (Bank of Bahrain and Kuwait) (<http://www.bbkonline.com/Pages/default.aspx> )
5. Future Bank Bahrain (<http://www.futurebank.com.bh/index.asp> )
6. Ithmaar Bank Bahrain (<https://www.ithmaarbank.com/> )
7. Khaleeji Commercial Bank (<http://www.khcbonline.com/> )

8. National Bank of Bahrain (<http://www.nbbonline.com/>)

## **RESEARCH OUTCOMES**

The outcomes of the research are presented in the form of recommendations. The analysis of this research also provides comprehensive discussion of the outcomes resulted from the survey conducted in this research.

## **INTERNET AND ITS ROLE IN ONLINE BANKING SERVICES**

Internet is one of the fast growing areas in 21st century which helped in developing technical infrastructure. The rapid growth of the internet applications changed the way we communicate and conduct other businesses in our day to day life. The growth of internet and other mobile applications also raised concerns for security elements particularly when dealing with online banking services and other sensitive electronic financial information. The need for appropriate security measures is critical as the influence of information technology and other mobile network devices on our society and its individuals goes far beyond than establishing basic information infrastructure.

Electronic business offers greater opportunities for business development throughout the world and many areas still need to be explored. However, there are serious concerns and threats available as cyber attacks now have the potential to affect the growth of the business particularly in the sector of online banking services. According to an IBM recent research of 350 companies in 11 countries, Bahrain is not included, \$3.79 million is the average total cost of data breach which is 23% increase in the total cost of data breach since 2013 (IBM, 2015). However, the researcher needs to consider the case of Bahrain in this study. Bahraini businesses are unprepared in the event of a major cyber assault as companies receive about 3000 cyber threats per month (Al-Bawaba, 2016).

To understand the security concerns and its needs for appropriate measures, ones need to understand the methods and tactics been adopted by cyber fraudsters to gain unauthorized access to steal financial information and use them later for fraudulent activities. These methods and tactics are discussed in further sections of this research.

## **IDENTIFY THEFT**

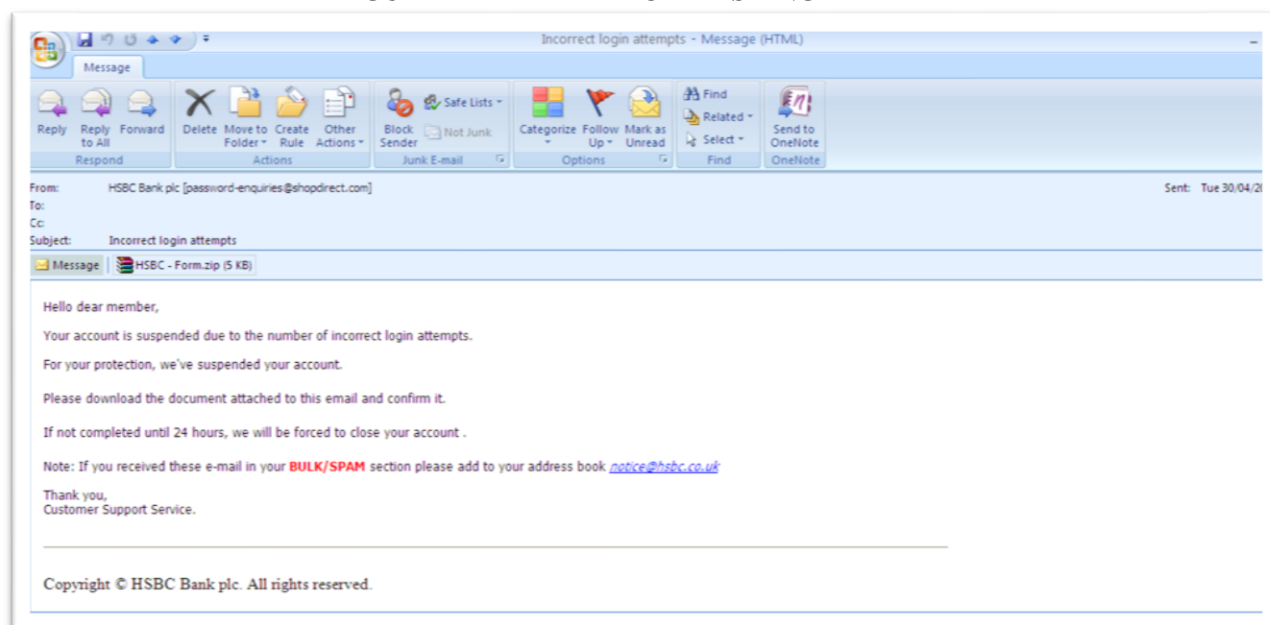
Using someone else identity such as name, date of birth, address for fraudulent activities is one of the common tactics adopted by cyber criminals when dealing with electronic businesses particularly online banking services. Information obtained through identity theft by cyber criminals can later be used for many purposes such as opening new bank accounts; obtaining credit card or loans and receiving state benefits. Identity theft is one of the world's fastest growing crimes and the Kingdom of Bahrain is one of the victims of identity thefts crimes. In March 2015, Bahrain probes mobile phone 'identity theft' cases where 10 expats were banned from travel due to this crime (Townsend, 2015).

## **PHISHING**

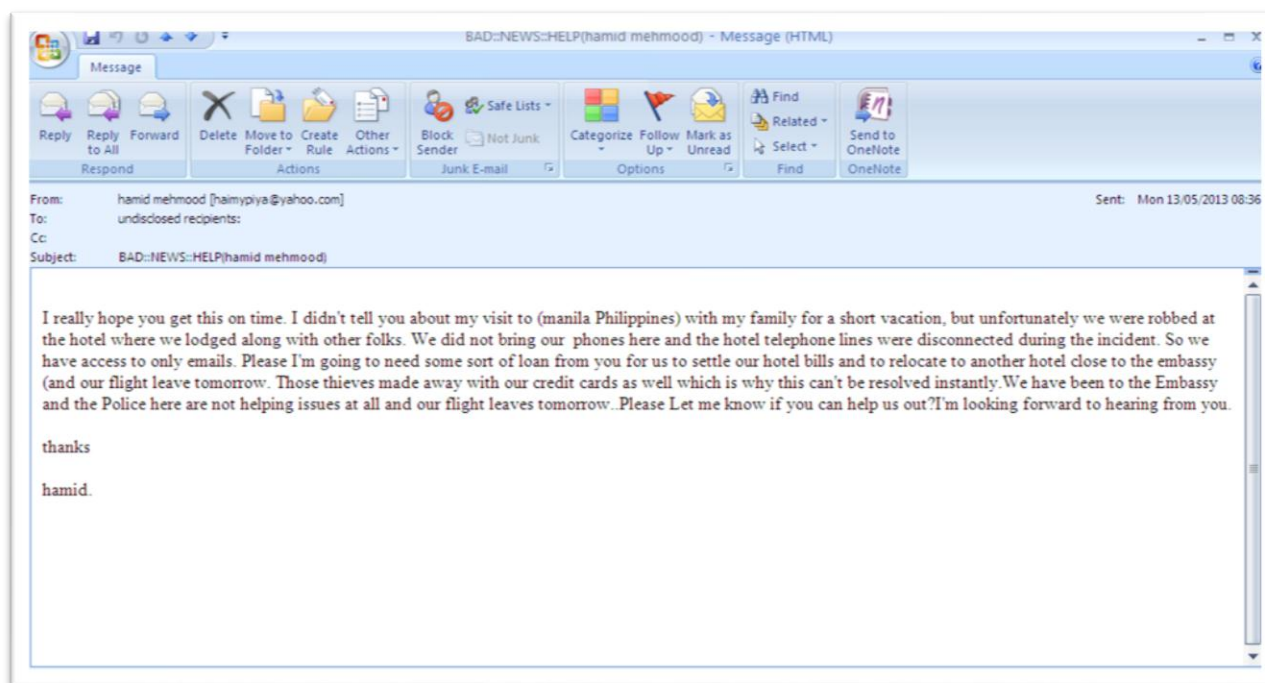
Phishing are tactics adopted by cyber criminals and fraudsters to make victims disclose their personal and other secret financial information. For phishing, there are many tactics which are used by cyber fraudsters but the most important tactics is sending a phishing email to online banking customers by pretending that a legitimate company/organization is offering electronic services. A 'spoofing site', computer fraudsters designed website similar to the legitimate websites of financial institutions, can also be used for the purpose of phishing activities and stealing financial information of the online banking customers. The protection of online banking data is becoming difficult in today's age of mobile applications as it was found that researchers at Websense Security Labs have stumbled upon a password-stealing Trojan that uses sophisticated DNS redirection techniques to dodge server shutdowns and hijack online banking data (CRIC, 2005). Phishing via mobile, computer applications and social media sites are the common platforms which are regularly used by computer fraudsters. It was reported by AFCC, Anti-Fraud Command Center, and that the total number of phishing attacks cost \$4.5 billion of loss in the year 2014 (RSA, 2016). An example of the phishing emails is provided in Figure 1 and 2 below, which was received by the author of this research on 30 April 2013 and 13 May 2013 respectively. The author had experience of many other occasions of the same instance.



**FIGURE 1 - EXAMPLE 1 OF PHISHING EMAIL**



**FIGURE 2 – EXAMPLE 2 OF PHISHING EMAIL**



## VISHING

Vishing or phishing using voice is a method of using fake call center using VOIP, Voice over IP, technique by computer fraudsters to acquire online banking customer's details and their financial data. To achieve the purpose an email system is used by fraudsters asking online banking customers to confirm their banking details and other information as process of security routine check at the phone number provided in the phishing email (Web, 2013).

## **HACKING**

Through hacking computer fraudsters can break into computer and computer networks to steal financial information which can later be used for unauthorized purpose. Different malicious software could be used for the purpose of hacking by computer fraudsters such as Trojan virus.

## **DENIAL OF SERVICES (DoS) ATTACK**

Denials of Service (DoS) attacks are attempts by cyber fraudsters to make network resource unavailable to its users. The nature of these attacks is so serious that Individual distributed denial-of-service (DDoS) attacks could soon take down not just one site, but any intervening service providers (DOPUK, 2013). *The costs of DoS attacks to critical infrastructure organizations can be significant. A respondent to the 2005 Australian Computer Crime and Security Survey reported a single-incident loss of \$8 million arising from a DoS attack (Unknown, 2006).* Online banking services must consider the seriousness of these attacks and cyber threats to its business growth and therefore serious measures should be taken to improve the level of security and to maintain sustained business growth. There is constant need to improve the layers of security to the applications of online banking services and to minimize the available threats coming from cyber space.

## **AUTOMATING ONLINE BANKING FRAUD**

Cybercriminals and computer fraudsters have now taken things a step further with the help of Automatic Transfer Systems (ATSs). A new system has been started for an Automating Online Banking Fraud system using in conjunction with SpyEye and ZeuS malware variants as part of WebInject files which is a text file with lot of JavaScript and HTML Codes (Kharouni, 2012).

## **MALWARE**

Malware (Viruses, Worms, Trojans and other threats) is the most significant threat available from cyber criminals to gain unauthorized access to user's accounts to steal their financial data and other sensitive information. The rapid growth in mobile devices such as SmartPhone and Tablet PCs leads to more development of the malicious software of Malware. Malware applications are used over the last few years by computer fraudsters to perpetrate hundreds of thousands of frauds against online consumers in business sectors particularly in online banking to draw off large amounts of money. Mobile Phone Malware is important to be considered here as some of the growing mobile platforms such as Android are the most targeted by malware authors (PandaLabs, 2012) and there is growing need to develop robust defenses against these sophisticated malware applications targeting online banking services and other financial institutions.

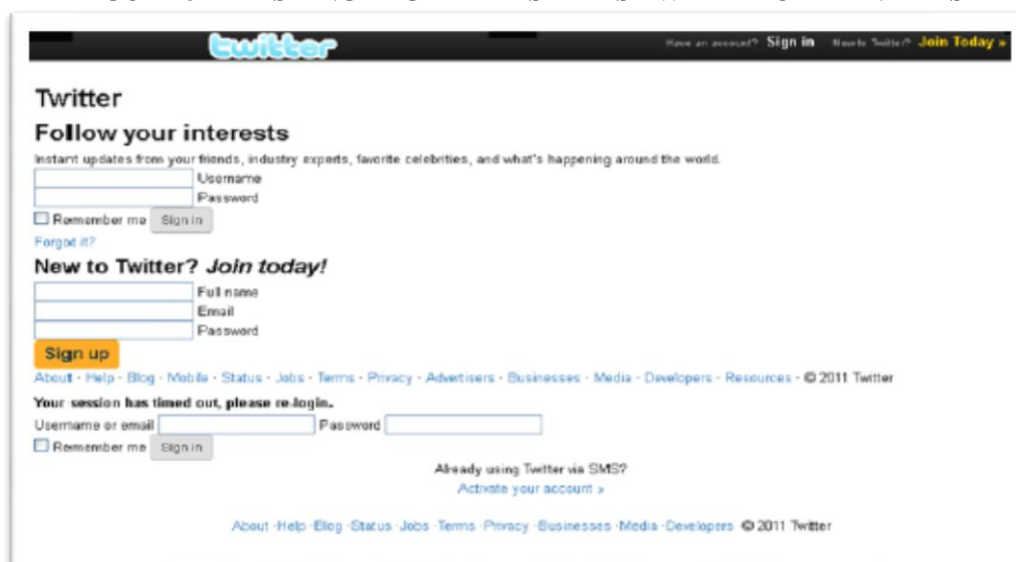
## **SOCIAL ENGINEERING**

Social Engineering is the art of manipulating people into performing actions or divulging confidential information. The social science discipline of social engineering is commonly used by computer fraudsters and cyber criminals to obtain financial data to gain unauthorized access to sensitive information.

## **SOCIAL NETWORKS**

Social Networks are the common platforms available for cyber fraudsters to access information shared by the account holders. The accessed information by cyber fraudsters can later be used for unauthorized purposes. These social networks platforms such as Facebook and Twitters allows user to send an instant message and during the process users could be redirected to some other website by providing a link by the fraudsters. An example of this is provided in Figure 4 below which informs the users that the session has timed out and asks that the user must login again. To make the phishing scam look as real as possible, all the links displayed on the page are actually Twitter links except for the "Sign in" and "Sign up" buttons, which will transmit the user data to the attackers (PandaLabs, 2012).

**FIGURE 3 – PHISHING PAGE THAT STEALS TWITTER CREDENTIALS**



Source: Extracted from (PandaLabs, 2012)

## **MOBILE PHONE AND OTHER ELECTRONIC GADGETS**

The use of smart-phones and other electronic gadgets such as Computer Tabs becoming common practice in today's electronic age. Security experts are predicting serious threats from cyber criminals and computer fraudsters on the available platforms of smart-phones and computer tablets. The increase in customer accessing online banking services and application through mobile devices and the available threats must be considered seriously by the financial organizations and online banking services to make sure that they are skilled to operate their services on as many of these new platforms as possible.

## **THE ARRIVAL OF ELECTRONIC MEDIA PLATFORMS**

People are using more sophisticated browser enabled platforms in their homes now. These include media streaming devices and internet based or smart televisions offered by many manufacturers. An example of Google TV is there too. Accessing internet via these platforms also create security concern for consumers. The platforms can easily allow cyber criminals and fraudsters to manipulate variety of physical devices through controlled applications. Consumer education and awareness is becoming more important on how to best utilize and access these electronic media platforms.

## **THE KINGDOM OF BAHRAIN- BANKS POLICIES AND ADDITIONAL SECURITY MEASURES**

In fact, it is very difficult to cover all the aspects of security measurements when dealing with electronic banking in the Kingdom of Bahrain as improving the level of security involves both physical and logical security. However, the author of this research is interested in security measurements along with the customer's behavior in regard to online banking. Further, this study is limited to 8 high streets banks in the Kingdom of Bahrain and therefore, discussion in the further sections illustrate the case study of these chosen online banking services only.

## **CASE OF CHOSEN BANKS IN THIS RESEARCH**

The research in this study found that security is considered very seriously by the online banking services in the Kingdom of Bahrain. However, no extra measurements are taken when dealing with online banking services. The only applied security mechanism which is called the 3D Secure Service. The service is available for the Master and Visa card holders only. The aim of the service is to protect Bank customers against unauthorized use of cards when they shop at participating online merchants. This mechanism is protected through personal customer's password giving them an extra layer of security and assurance that only card holders can use the card when dealing with



merchants. If registered for this service, bank customers must need to provide the personal message in the form of password to confirm their identity with the bank before accomplishing the transaction.

### **Case of HSBC, the Kingdom of Bahrain**

For the purpose of two factor authentication process HSBC provides its customers a key fob and card reader which generates a unique key during the time of online banking transactions. The unique key is also used by the time of login to online banking by the customers of HSBC. This is an example of providing extra security while providing online banking services. However, the HSBC is not the bank of Bahrain.

**FIGURE 4- HSBC SECURITY CARD READER AND KEY FOB**



As mentioned, provision of 100% security is never possible in online banking sectors. However, it is important that financial institutions must consider this factor seriously. Therefore, extra measures must be considered when dealing with online banking. This will alternatively, improve the confidence and trust of online banking customers.

### **RESEARCH METHODOLOGY – PHILOSOPHY AND APPROACH**

The research questions and objectives must be delineated in the research philosophy and approach. Looking at the research philosophy (Saunders et.al, 2009) the four main factors realism, positivism, pragmatism and interpretive must be considered. The author of this research prefers to use the pragmatism philosophy where research hypothesis and other theories are carefully formulated. This alternatively helped in beginning with the wide-ranging ideas. Also, with inductive approach of the research, the researcher initiated observations of individual cases. Based on all observations and wide-ranging idea the researcher analyzes the data of this research which further helped in recommendations of the research.

### **RATIONAL FOR PRAGMATISM PHILOSOPHY**

As mentioned by (Saunders et al, 2009) the pragmatism is one of the most important philosophies in the research. By the help of this approach, a researcher can conclude proper and significant answers to his research questions. This allows researcher to use the observations and discussed findings for that reason. The chosen philosophy of the research helped the researcher to collect different views from different channels and to analyze them further for the interpretation of the research data. The author is therefore believed that the chosen philosophy is the appropriate for his research and will helped in collecting and analyzing the data in appropriate manner.

## **RATIONAL FOR INDUCTIVE APPROACH**

The author of this research selected the inductive approach compare to deductive approach. The reason for not selecting the deductive approach because the approach is more suitable for the facts and arguments based on accepted principles, rules and regulations or laws. In contrast the inductive approach will help researcher to move from specific to generalization like bottom-up approach. This will help in clear understanding and the perceptions of insights of the target population of this research.

## **PRIMARY AND SECONDARY DATA OF THE RESEARCH**

It is important to have discussion about the primary and secondary data of this research. The conducted research contains both primary and secondary data. By the help of secondary data, the researcher tried to understand the relevant work in the field of cybercrimes and online banking services in the Kingdom of Bahrain. However, it is important to be mentioned that much needs to be written in the area of cybercrimes and online banking services as very little consideration has been paid to the issues of security by the security developers and researcher in Bahrain. The primary data of this research is collected through the survey of the research. The survey was accomplished through the online questionnaire where every question was selected by the author carefully to make sure that research objectives are achieved and recommendations could be structured at the end of the survey.

## **DATA COLLECTION METHODS**

It is critical for every researcher to get appropriate answers to their research questions and therefore the data collection process and methods play an important role in the research process as a whole. As mentioned above, primary and secondary both data is used in the process of this research. The research primary data is collected through questionnaires while the secondary data is collected through several sources such as academic journals, articles and conference papers. The first section of the research questionnaire contains respondent's personal data such as their gender, age group and employment status. This part will help in understanding the behavior of online customers based on the categories selected. The second part of the questionnaire contains research questions that need to cater by the researcher to respondents of the survey.

## **RESEARCH QUESTIONNAIRE AND TARGET POPULATION**

Initially the research questionnaire was developed and carefully analyzed by the author of this research. The questions of the survey were carefully selected to align with the objectives of research. The author approach was to target general population to understand the behavior of online customers. However, it was decided to conduct the survey in the university environment where author is employed. Then further the author contacted employees from banking industry. This approach helped in collecting data both from students and staff members of the banking industry and university which further helped in the research conclusion. However, students and staff members from other universities and different organizational employees especially from banking security sectors also contributed in the survey of this research.

The questionnaire of the research contains both demographic and research questions. The author of this research took extra measurements to build questionnaire to make sure that a reliable and unbiased questionnaire could be designed in order to find answers to the research questions and objectives. Therefore, a well-structured closed ended questionnaire was designed for the current research in this paper. The questionnaire was applied through online tool and the link was distributed to target population of the survey. From the responses collected, it was found that all respondents showed elevated interest in the survey and this further leads to the success of the research conducted.

## **DATA VALIDITY THROUGH PILOT TESTING**

For the sake of strength, reliability and uniformity it was critical to conduct pilot testing for the survey to ensure data validity. For the objective to be achieved a trial phase was conducted by the author and the questionnaire was reviewed by the selected respondents to avoid unexpected errors. This further leads for the collection of valid data from the respondents of the survey. After minor changes, the author approached the survey respondents to collect the data. With the help of tables and charts, the author easily and precisely measures the demographic information of the survey respondents. The statistical tool used for the analysis of this research helped in confirming the data to be on the right path.

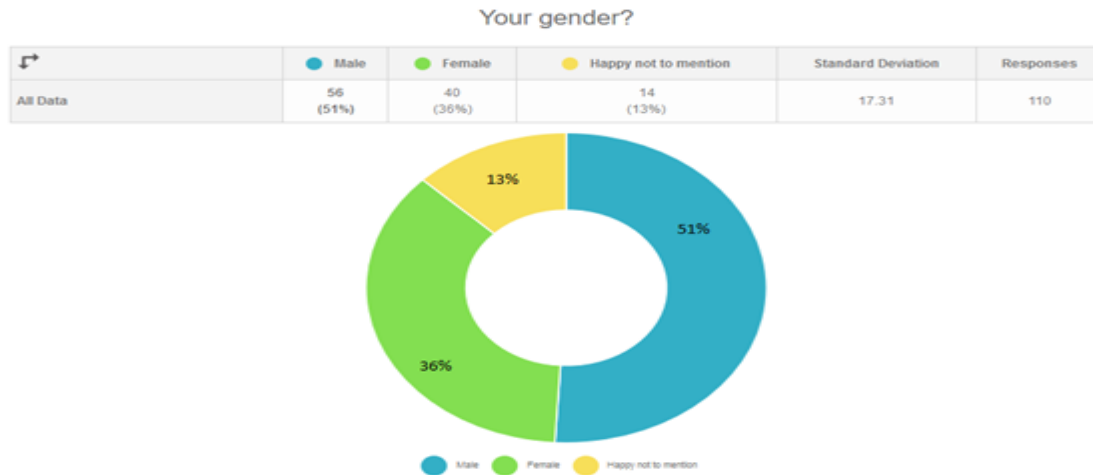
## ETHICAL CONSIDERATION

The ethical consideration is critical for the survey of this research as the research was conducted in university and banking environment. It was important to approve the research questionnaire from the research committee. Once approved, the tool was applied successfully as per research objectives. The ethical consideration of the research helped in formatting the success of this research. The researcher took extreme care not to exploit any respondent in terms of information as the questionnaire was relevant to online banking services and the objective was to measure the behavior of the end user. The researcher, therefore, ensure the anonymity and confidentiality of the respondents. All the respondents willingly participated in the survey.

## FINDINGS AND ANALYSIS

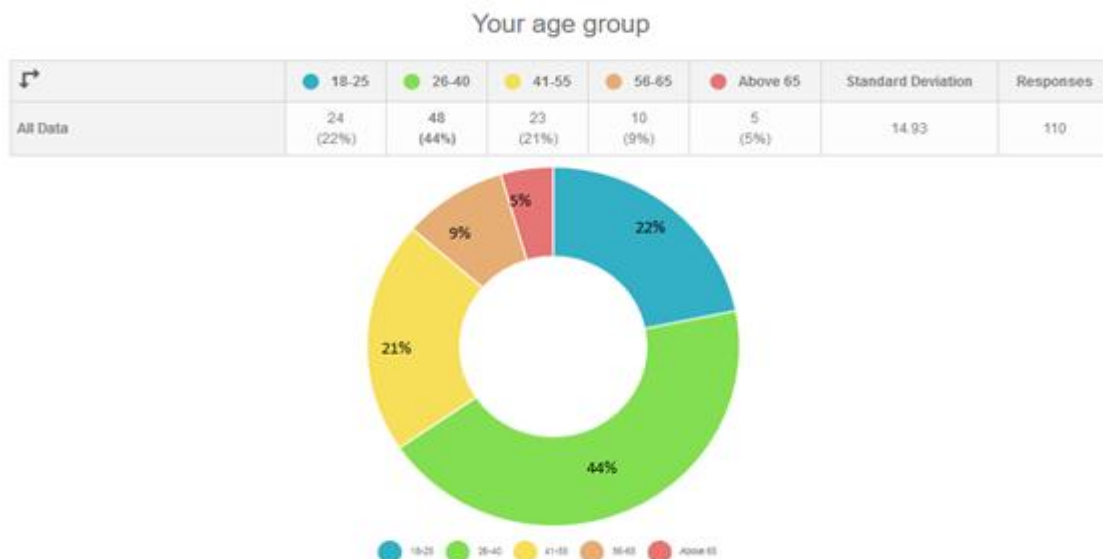
The findings of 21 survey questions are analyzed in the further sections of this research.

**FIGURE 5 – GENDER OF SURVEY RESPONDENTS**



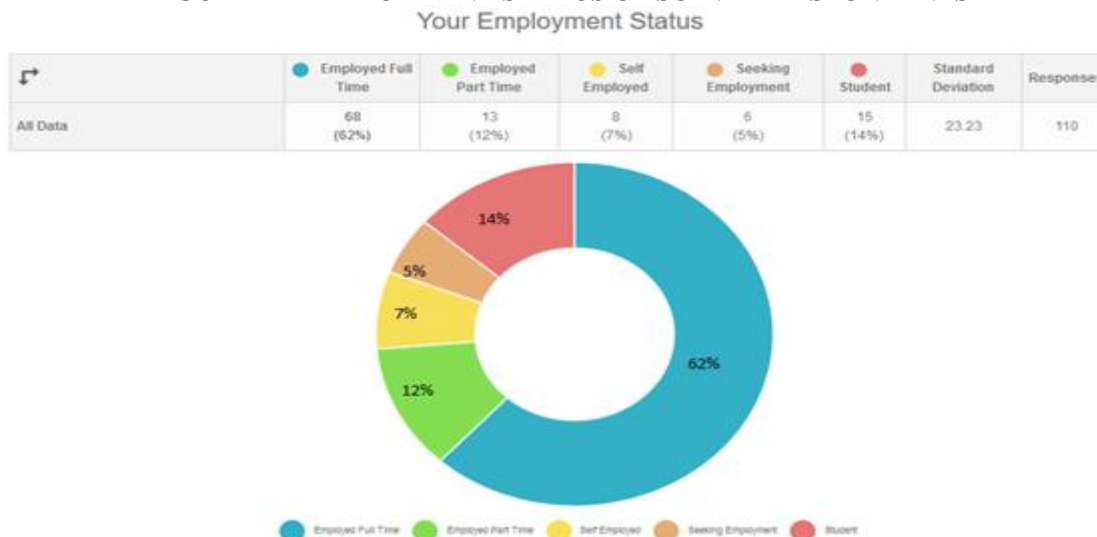
The questionnaire of this survey was equally distributed to all target population regardless their gender. As shown in Figure 5, out of 110 respondents 51% male and 36% female participated in the conducted survey of this research. The other 13% respondents didn't mention their gender. In general, male participation was higher compare to female respondents and the standard deviation of the respondents was noted as 17.3 in total.

**FIGURE 6 – AGE GROUP OF SURVEY RESPONDENTS**



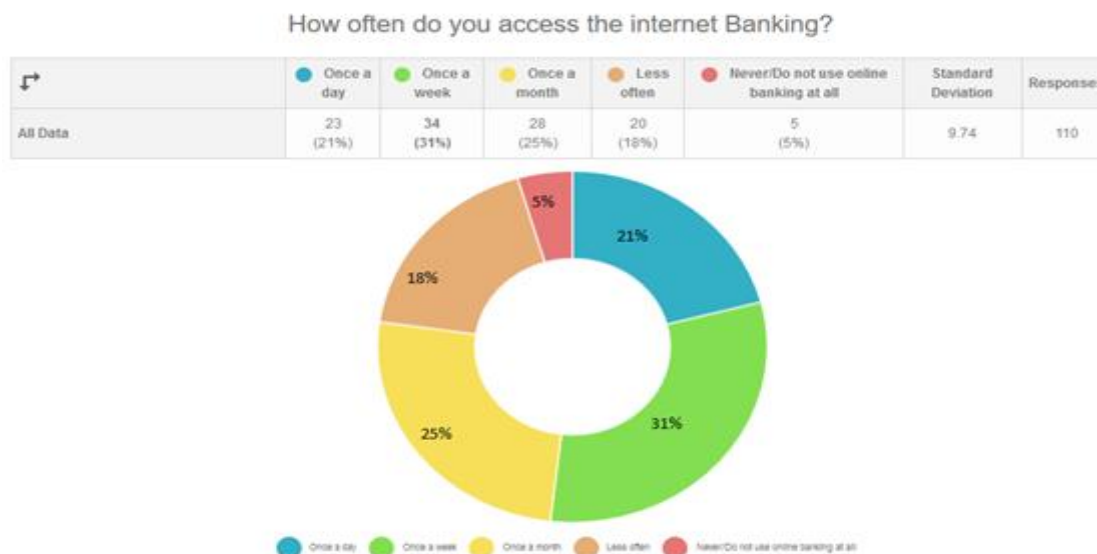
As shown in the above Figure 6, 44% respondents between the ages of 26-40 participated in the survey of this research. This proves elevated interest taken by the middle age people who deal with the online banking services. However, the response from the young respondents such as 18-25 and 41-55 years of age were highly substantial i.e. 22% and 21% respectively. Only 9% respondents between the age group of 56-65 and 5% above 65 years old contributed in the survey of this research. Overall, it could be concluded that respondents from all age groups showed high interest in the survey and participated in the successful completion of this research.

**FIGURE 7 – EMPLOYMENT STATUS OF SURVEY RESPONDENTS**



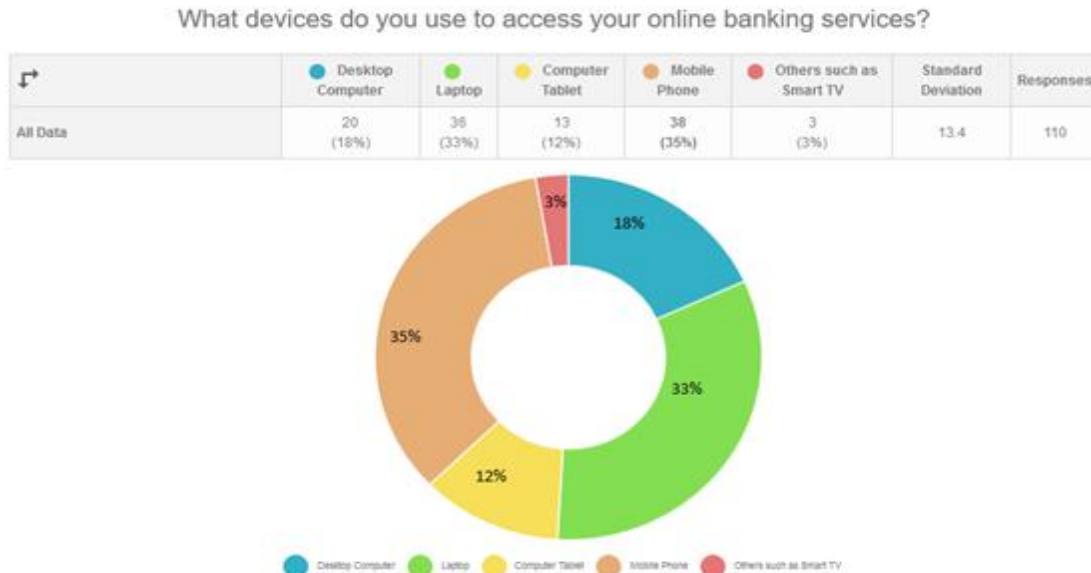
As per Figure 7 above, 62% respondents of this survey are employed full time while only 12% respondents are part time employees who deal with online banking services. Only 7% respondents are doing their own business or they are self-employed while 5% respondents are in the process of seeking employment. Out of 110 respondents only 14% are students and not involved in any employment. However, their behavior is important to understand in regard to online banking services. It is further important to understand that this survey was conducted in university environment along with the banking industry where majority of the students are employed full time or part time in different industries across the Kingdom of Bahrain. Some of these students are in the process of seeking employment. Therefore, it would be more appropriate to consider that students are the highest participants of this survey regardless their other status in the existing industry.

**FIGURE 8 – FREQUENCY OF USING ONLINE BANKING**



For the question above, when users were asked how often they use their online banking services? Out of 110 respondents, 21% confirmed that they use online banking services every day. The other 31% confirmed that they use online banking once a week. The 25% respondents confirmed that they are using online banking services once a month while 18% confirmed that they are less often using these services. Also, 5% respondents confirmed that they do not want to use online banking services as they are not comfortable with it. The response collected for this question shows that high majority of respondents using the online banking services.

**FIGURE 9 – DEVICES USED FOR ACCESSING ONLINE BANKING**



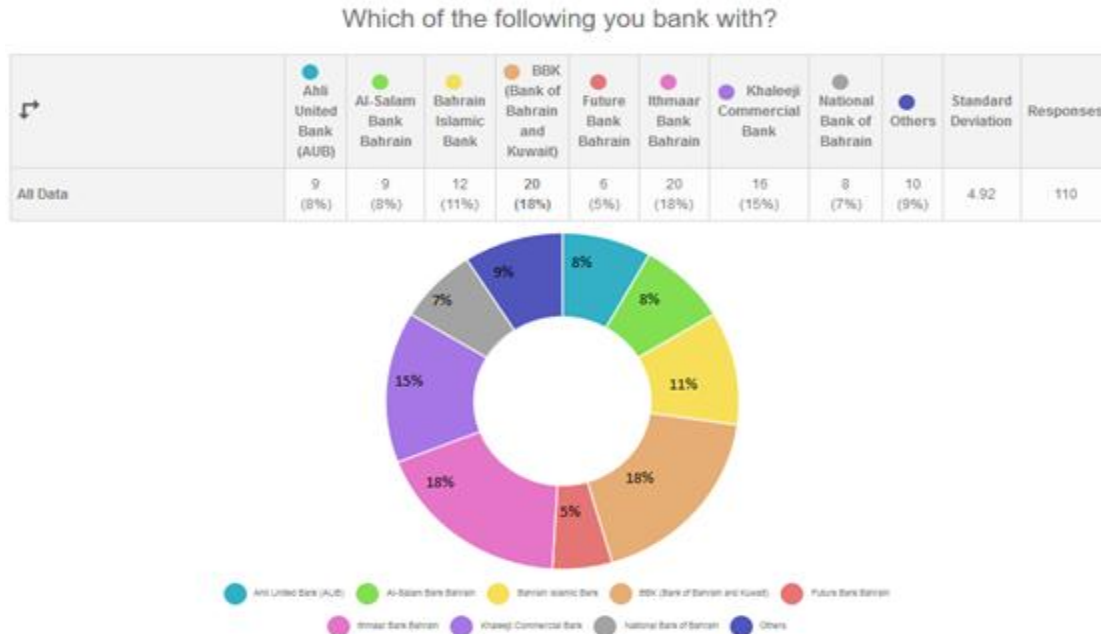
For the question above, 18% respondents of the survey confirmed that they are using their desktop computers while dealing with online banking services. It was noticed that 35% users use the services by their mobile and 33% respondents use their laptops to access online banking. Also, 12% respondents confirmed that they use their computer tablets and 3% users use other devices to access online banking services.

**FIGURE 10 – NUMBER OF ACTIVE BANK ACCOUNTS OF SURVEY RESPONDENTS**



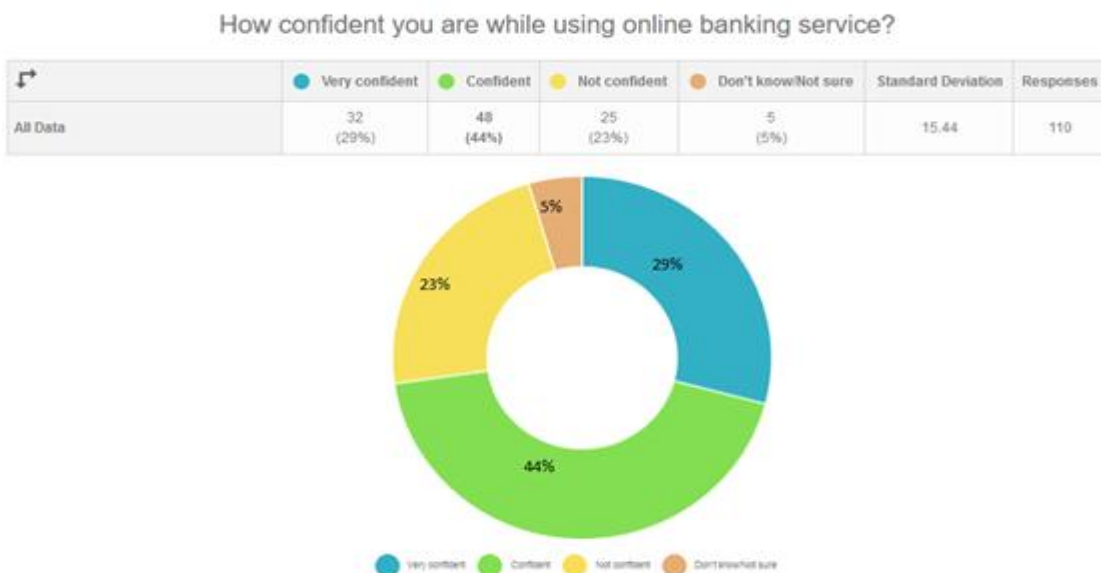
The question above shows the total number of active bank accounts the respondents having with different banks in Bahrain. It was confirmed by the 23% respondents only that they are having only one active account and the other 77% confirmed that they got more than one active accounts. This means that they are dealing with different online banking systems. The behavior of these online banking customers is therefore important to understand to further measure the effects of cyber crimes on business growth.

**FIGURE 11 – ASSOCIATED BANK OF SURVEY RESPONDENTS**



The above question confirmed that the selected banks for the study of this research are the popular banks in Bahrain. As per the data collected, 18% respondents confirmed their banking with BBK and other 18% with Ithmar Bank of Bahrain. 15% respondents confirmed their banking with Khaleeji Commercial Bank and 11% respondents confirmed that they do banking with Bahrain Islamic Bank. 8% respondents do banking with Al-Salam bank of Bahrain, another 8% with Ahli United Bank and 7% do banking with National Bank of Bahrain. However, 9% respondents of the survey conducted for this research confirmed that they do banking with other banks in Bahrain.

**FIGURE 12 – RESPONDENTS CONFIDENCE LEVEL OF USING ONLINE BANKING SERVICES**





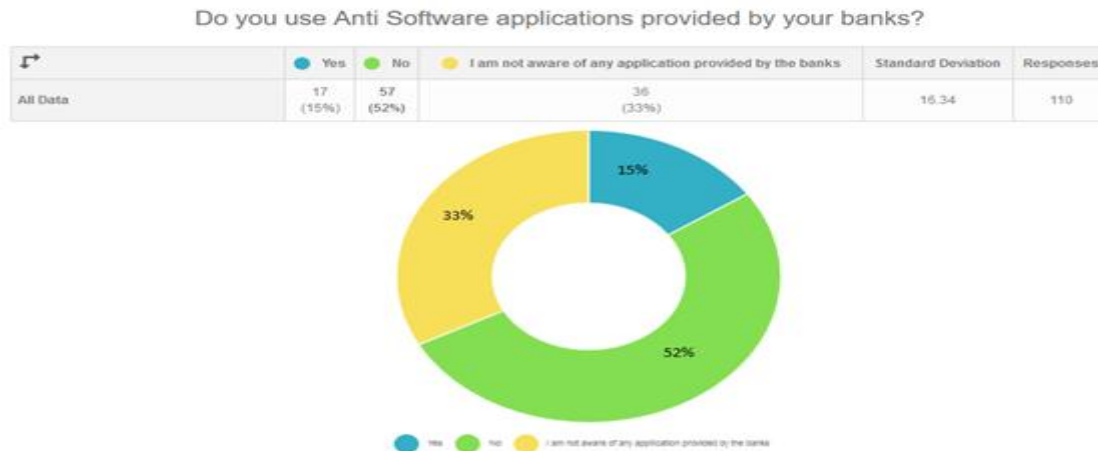
As shown in Figure 12, 73% respondents confirmed that they are very confident or confident when dealing with online banking services. 23% respondents confirmed that they do not have any confidence when dealing with online banking services while other 5% confirmed that they are not sure about the level of confidence on this matter. However, it was confirmed by the majority of the respondents that they use online banking services confidently and perform day to day transactions through different devices.

**FIGURE 13 – RESPONDENTS AWARENESS OF AVAILABLE CYBER THREATS**



The above question proves the level of awareness of the respondents in regard to online banking services and available cyber threats. As shown in Figure 13, 37% respondents are aware of the computer hacking, 6% are aware of phishing while other 6% confirmed that they got awareness about vishing (phishing over VOIP). Out of 110 respondents, 13% confirmed their awareness about identify theft and 5% confirmed about DoS attacks. 1% respondents confirmed their awareness about social engineering. However, it is important to note that 31% respondents are aware about all the crimes and cyber threats mentioned in the survey. As employees from banking sectors were involved in the survey of this research, it is more likely that these respondents deal with these crimes on daily basis and therefore they got knowledge and awareness about these crimes and cyber threats.

**FIGURE 14 – THE USE OF ANTI SOFTWARE APPLICATIONS**

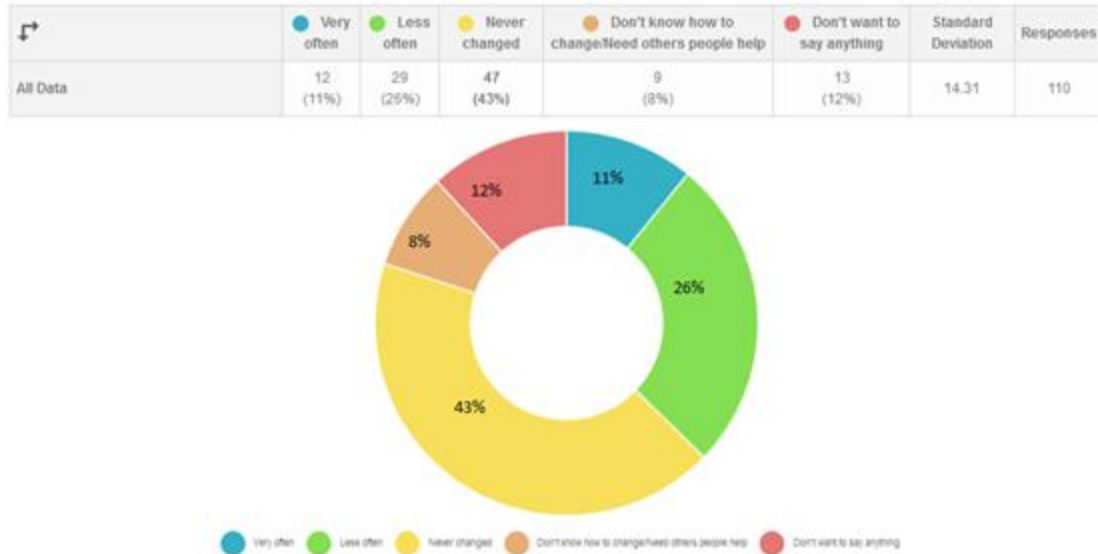


When the survey respondents were asked about the use of software applications to keep their online banking services in secure environment, it was confirmed by only 15% that they use such applications. The other 52% respondents who deal with online banking services do not use any application software for security or no application

software is provided by the banks they deal with. Also, 33% respondents are completely unaware about such applications available from the banking sectors.

**FIGURE 15 – FREQUENCY OF CHANGING PASSWORDS FOR ONLLINE BANKING ACCOUNTS**

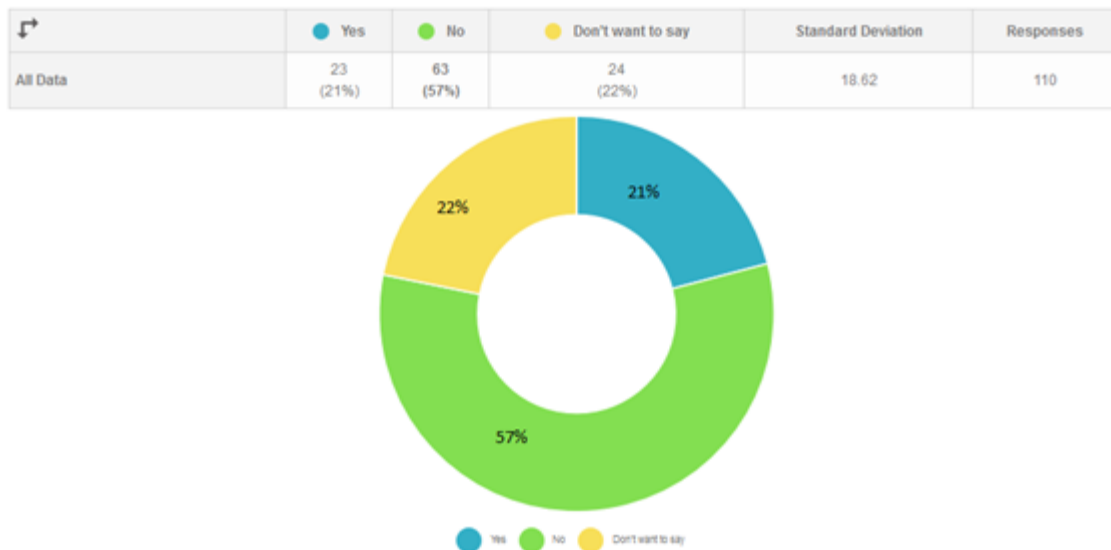
How often you change the password of your online banking when accessing your online banking account?



As shown in Figure 15, only 11% respondents regularly change their password to keep their online banking secure from online threats. 26% respondents hardly change their passwords while 43% never changed their passwords at all. The other 8% users are not even aware how to change their password of online banking accounts.

**FIGURE 16 – VICTIMS OF ONLINE BANKING FRAUDS**

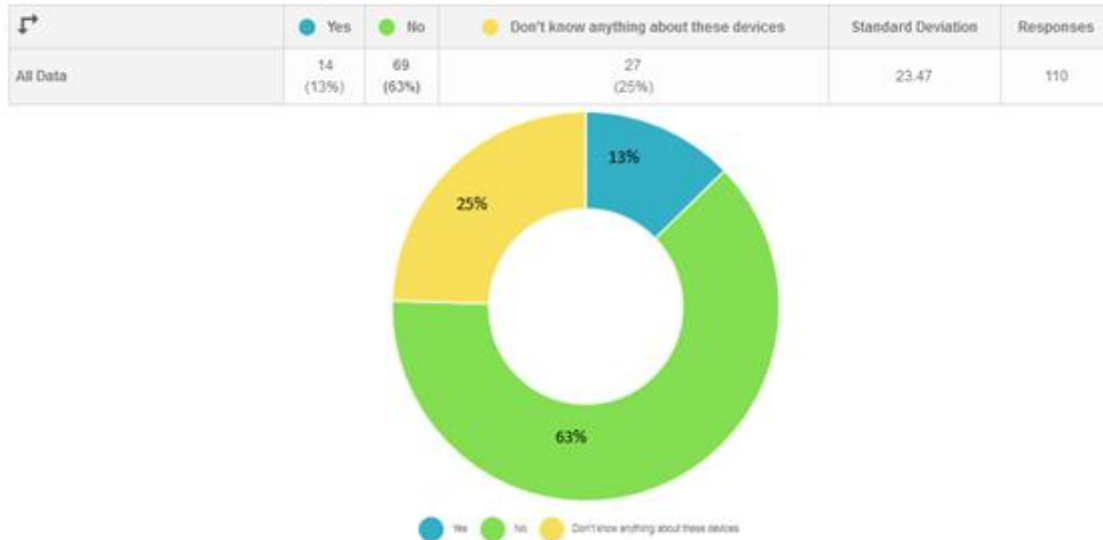
Do you ever become a victim of online banking fraud?



As shown in Figure 16, 21% respondents of this survey confirmed that they became victims of online banking services. The other 57% never had an experience of cyber crime attacks while 22% respondents didn't want to mention about their experience in regard to online banking services.

**FIGURE 17 – THE USE OF ADDITIONAL SECURITY DEVICES**

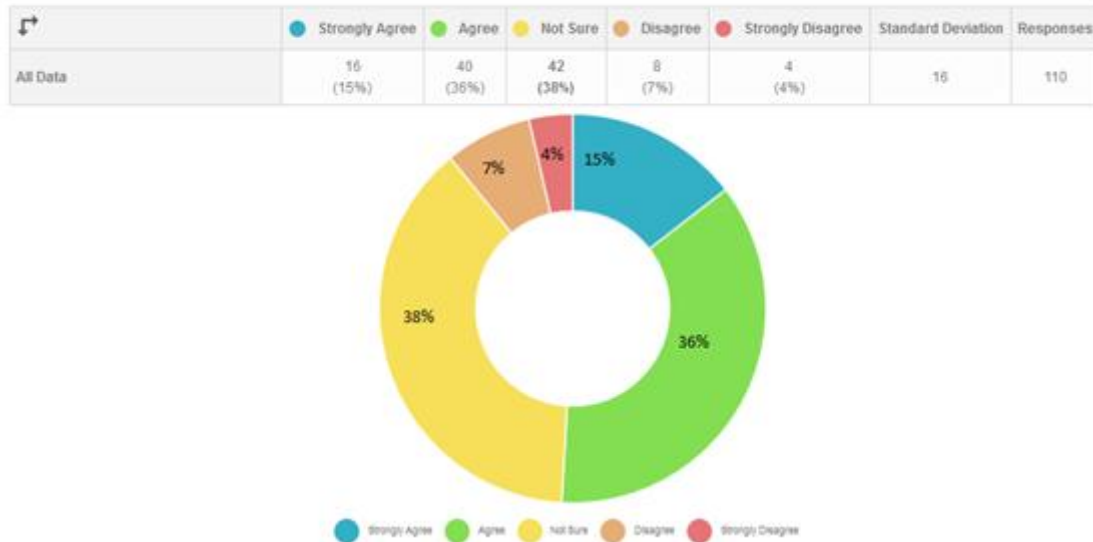
Do you use any additional security device such as security card readers or key fobs provided by the banks for online transactions?



For the additional security devices such as card readers and key fobs to generate unique numbers to accomplish online transitions, out of 110 respondents 63% respondents confirmed that they do not use such services while other 25% respondents are completely unaware of such device which helps to improve the security level of online banking services. Only 13% respondents confirmed the use of such devices.

**FIGURE 18 – RESPONDENTS AWARENESS OF INFORMATION SECURITY THREATS**

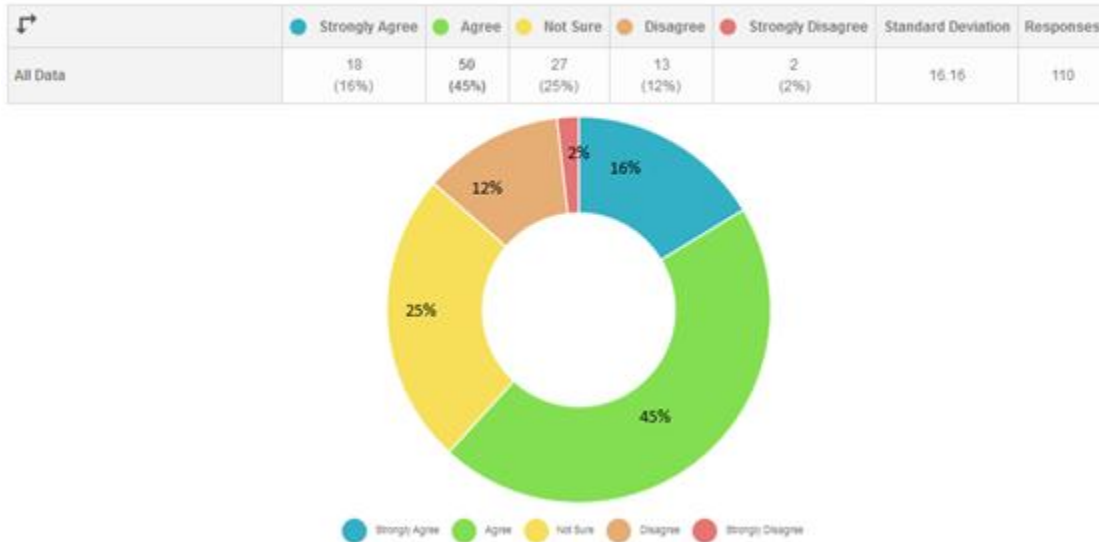
I am completely aware of the information security threats available to individuals and financial institutions/online banking services.



As shown in Figure 18, 51% respondents confirmed that they are aware about the security threats available to individuals and financial institutions or online banking services. However, 38% respondents further confirmed that they are not sure about such threats. Other 11% got no or little awareness about the availability of these threats to financial institutions and individuals.

**FIGURE 19 – RESPONDENTS PERSONAL EXPERIENCE OF RECEIVING EMAILS ASSOCIATED WITH CYBER THREATS**

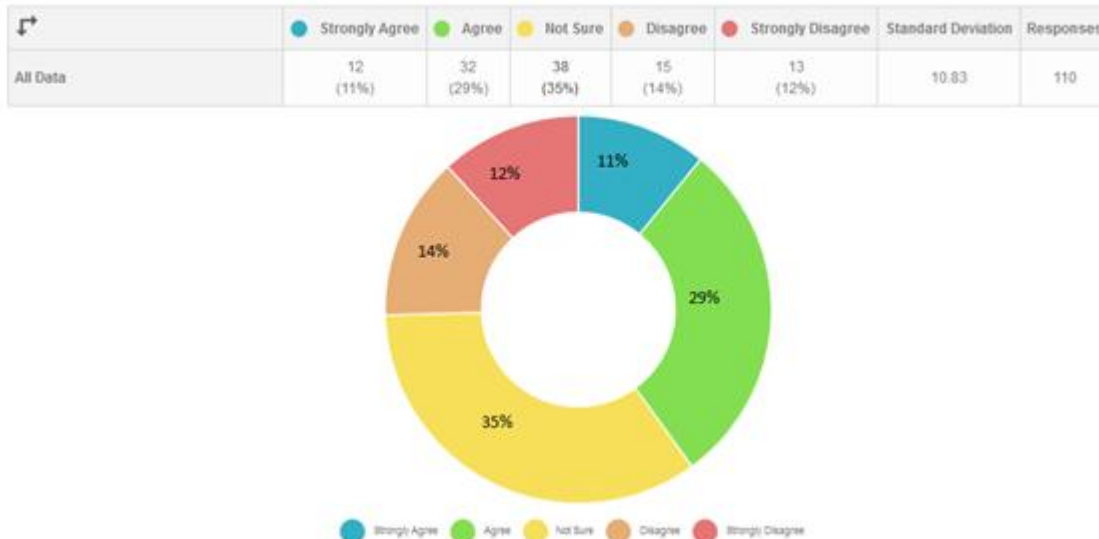
I have experience of receiving personal emails related to cyber threats and other online security.



As shown in Figure 19, out of 110 survey respondents 51% confirmed that they got personal experience of receiving forge emails by computer hackers and criminals to access their financial information. 25% respondents are not sure about such emails while other 14% never had an experience of such messages.

**FIGURE 20 – RESPONDENTS ABILITY TO IDENTIFY AND HANDLE INFORMATION SECURITY THREATS**

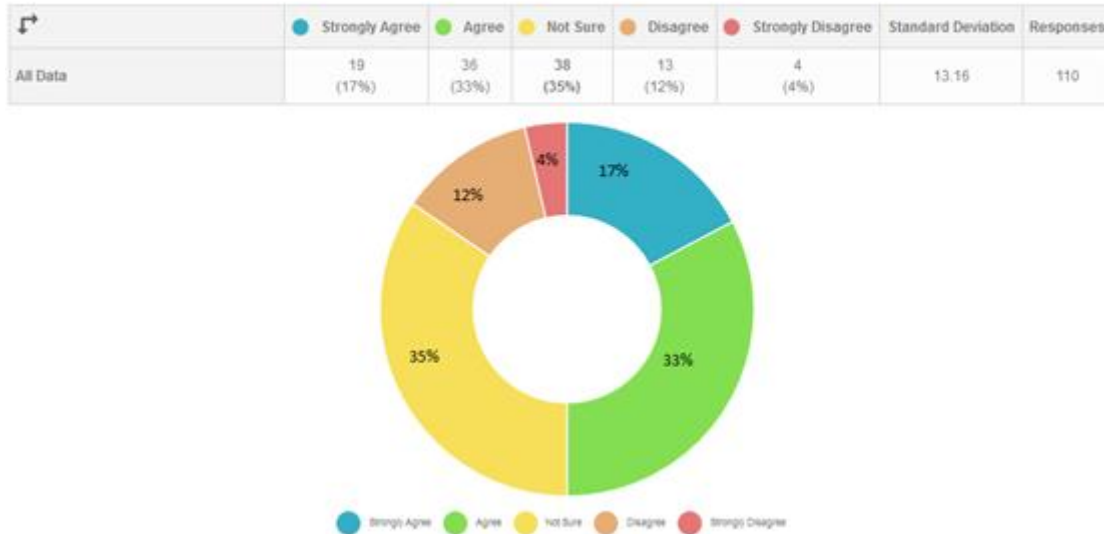
I am able to identify and handle information security threats myself.



It was confirmed by the 40% of survey respondents that they are able to identify information security threats and further they got the ability to handle with such threats. However, 35% survey respondents are not sure that they can manage such threats. 26% respondents as per the Figure 20 above cannot identify such threats and also do not have the ability to handle such threats.

**FIGURE 21 – RESPONDENTS LEVEL OF EXTRA CARE DEALING WHEN DEALING WITH ONLINE BANKING SERVICES**

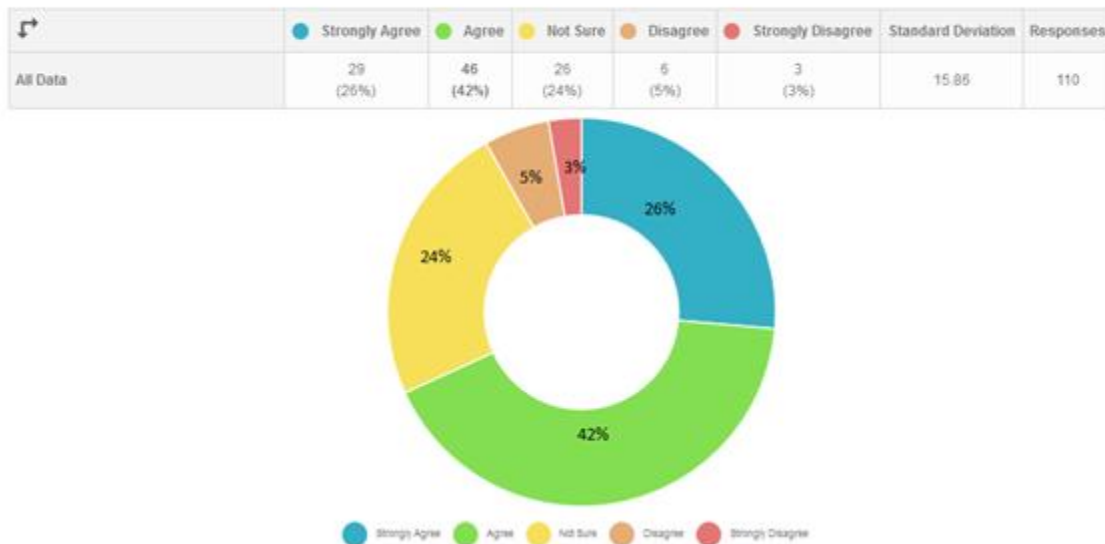
I take extra measurement while doing online banking and dealing with other sensitive information on internet.



For the question above, it was confirmed by the 50% respondents of the survey that they take extra care when dealing with online banking services. Further 35% respondents are not even sure while other 16% do not care any measurements when dealing with online banking services.

**FIGURE 22 – INDIVIDUAL'S ROLE IN REDUCING INFORMATION SECURITY RISKS**

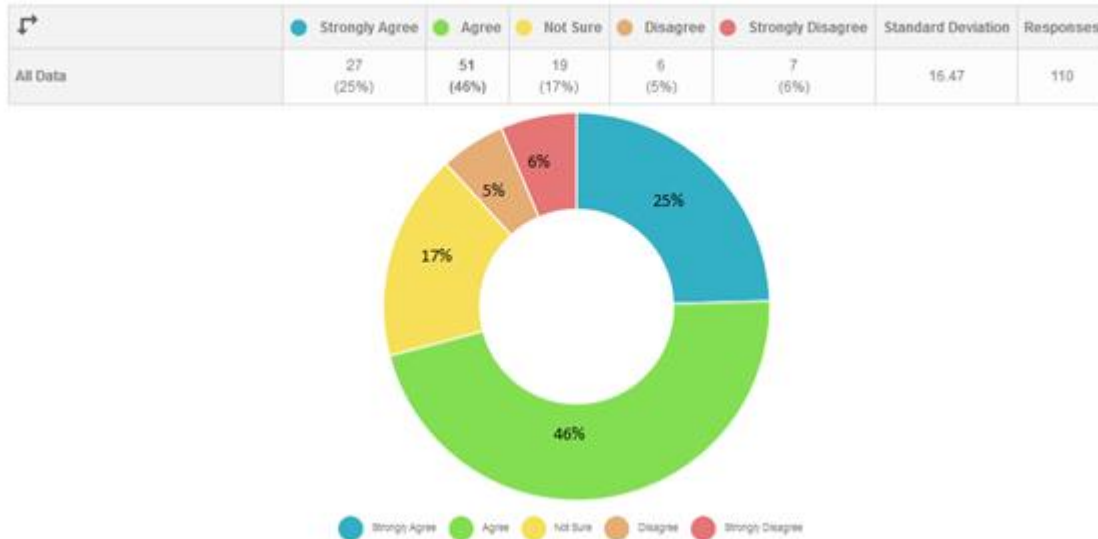
The role of every single individual/banking customer is important to reduce information security risks.



As illustrated in the Figure 22 above, 68% respondents of the survey are agreed or strongly agreed that the role of every single individual is important in reducing information security risks. The other 24% respondents are not sure while 8% do not agree with this statement.

**FIGURE 23 – MANAGING CYBER THREATS THROUGH APPROPRIATE TOOLS**

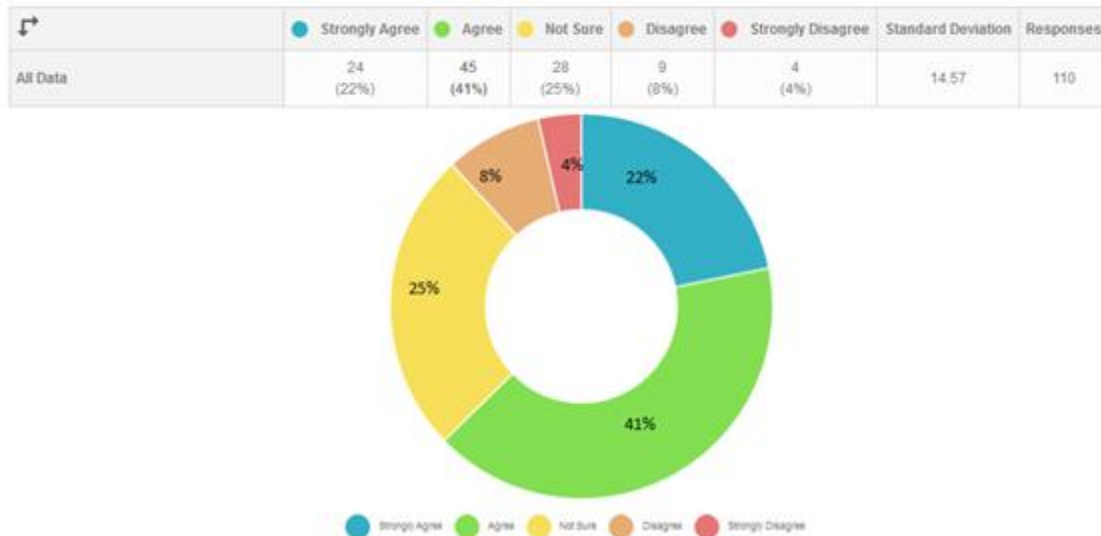
Information Security and other cyber threats could be managed by using appropriate tools and safeguards software/applications.



Out of 110 respondents, 71% agreed or strongly agreed that information security and other cyber threats available to individuals and financial institutions could be managed by appropriate tools. However, 17% respondents are not sure about such tools while other 11% respondents think that this cannot be managed by tools only.

**FIGURE 24 – MAXIMUM SECURITY POSSIBILITY OF ONLINE BANKING SERVICES**

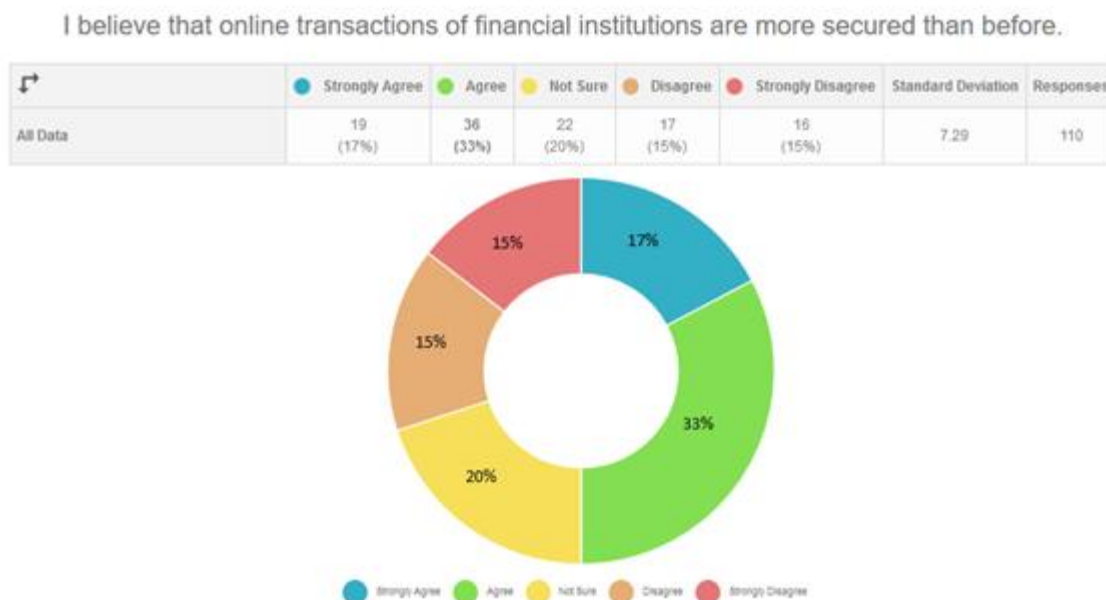
There is no possibility to provide 100% security to financial institutions as computer hackers and criminals are always two steps further than security managers.



For the maximum security to be achieved, out of 110 respondents of this survey 63% are agreed or strongly agreed that there is no possibility to achieve 100% security of online banking services. However, 25% are not sure about this statement while other 12% respondents believe that 100% security could be achieved.



**FIGURE 25 – EXISTING LEVEL OF ONLINE BANKING SECURITY**



As shown in Figure 25 above, 40% respondents are agreed or strongly agreed that current level of online banking transactions are more secure than previous security levels. 20% of the respondents are not sure while other 30% believe that these transactions are not secure as they were before.

## DISCUSSION AND CONCLUSION

The conducted survey of this research based on 110 responses made it possible to draw the conclusion of this research as per the objectives defined above. Both male and female respondents regardless the differences between their genders participated in the successful completion of the survey. The data was collected from university undergraduate and postgraduate students, staff members and employees from different banking sectors especially from BBK Bahrain and Khaleeji Commercial Bank of Bahrain. Further, respondents from all age groups participated in the survey of this research. The research found that majority of the respondents used online banking through different devices such as laptops, desktops and computer tablets. They also use mobile banking to access their financial information and to perform other transactions. It was also found by the researcher that majority of the respondents are keeping more than one active bank accounts and they use the online services of different banks and financial institutions. However, the security of these financial and banking organizations is another issue to be considered here when it comes to online banking services. Further, the research proved that the chosen banks for the case study of this research are the popular street banks of the Kingdom of Bahrain and therefore it is important to understand and identify the security issues when dealing with online banking services. The confidence level of the online banking users is measured and it was found that more than 70% users are comfortable when dealing with financial institutions and with associated services provided by banking industry.

When dealing with online banking and other services, it is critical that users must be aware about existing threats coming from computer fraudsters and criminals. Computer fraudsters use different techniques and methods such as computer hacking, phishing, vishing, identify theft, denial of services, social engineering and many more to steal the financial data of end users. It is therefore important that online banking customers must be aware about these techniques and methods used by computer fraudsters. However, only 31% respondents of the survey confirmed that they are aware about all the threats mentioned in the survey of this research. The author of the research further believed that because of the participation of the employees from the banking sectors it is more likely that they belong to the mentioned population above. This proves that almost 70% online customers got limited or no awareness about the threats available to individual and banking industry. This further opens doors for computer criminals and fraudsters to access unauthorized customer's information and to utilize them for their illegal activities and objectives. Previous research proved that Bahrain got the history of cyber-attacks alternatively affected the growth of business in the country. The spam fighter news 2006 reported that Bahrain and Kuwait both were targeted for phishing (SPAMfighter, 2006). Also it is important to understand that the current regulation have in place have

not caught up with developments of cyber space and that makes us totally vulnerable (Shaw, 2013). The banking sector in Bahrain is therefore need to increase this awareness among online banking users by introducing additional security devices and to make sure that the services provided by them are secured and the users are educated at the same time.

Banks such as BBK provides the ePin services which help online banking customers to access their retail banking, telebanking, mobile banking, E-statement and SMS banking but there is possibility that computer fraudsters can have access to these ePins which can further jeopardize the security system. The provision of online anti software applications for monitoring online banking transaction and access to banking services is a helpful tool that could be used to achieve the further layers of security. For example, in United Kingdom the bank of NatWest provides a free Rapport Security Software which protects online banking users when they access their online banking services (NatWest, 2016). However, the survey of this research found that 52% online banking customers are not using any secure application, provided by the banking industry in Bahrain, and other 33% are not even aware of that. This can further jeopardize the security of online banking services. As proved in the survey that more than 70% respondent agreed that information security and other cyber threats could be managed by using appropriate tools and other safeguards such as anti-software and applications.

The provision of only user name and passwords to access online banking services as in the case of Bahrain can easily jeopardize the security system of the financial institutions. It was confirmed by the 43% of the respondents of the survey of this research that they never changed their password of online banking services. Also, 26% online banking customer change their password less often and other 8% are not aware on how to change the passwords even. It is therefore, important for the banking industry in Bahrain to introduce three factor authentication systems by introducing additional security devices such as card readers and key fobs. It was found in the survey of this research that 63% user do not use any such services while other 25% are not aware even. Only 13% users confirmed the use of these devices but the author believes that it could be the case of HSBC or other foreign banks in Bahrain as some of them use three factor authentications when dealing with online banking services.

The survey of this research proved that online banking customer in Bahrain faced online banking frauds. It was confirmed by 21% of respondents that they are the victims of online banking services. Also, 22% respondents did not mention about their experiences and the author believes they may be victims of online banking frauds. This clearly shows that activity of computer criminals and fraudsters are available in the Kingdom of Bahrain.

As per the survey conducted, more than 60% respondents got the experience of receiving personal emails related to cyber threats and online banking. This shows that computer fraudsters and hackers are active in the country of Bahrain who regularly send these emails and use other social engineering tools to gain unauthorized access to steal financial data of the online banking users. The online banking users need to take further extra care when dealing with these services. However, more than 60% users are unable to identify and handle the existing information security threats. Also, about 55% users do not take any extra care when dealing with online banking services.

More than 60% respondents believe that there is no possibility to provide 100% security of the online banking services and the banking industry in Bahrain can never achieve the maximum security by its own and it is critical that every individual make sure that they deal with all financial transactions in secure online banking environment. However, 24 % respondents of the survey are not sure about this while other 9% does not believe on the individual's role to secure the banking environment. The banking industry in Bahrain has to take this seriously and make sure those individuals are aware about their personal role when dealing with online banking services. Also, a large population of the survey believes that online banking services are not as secure as before because computer fraudster and other hacking activities are getting increased day by day and therefore pose new threats to the banking industry in the Kingdom of Bahrain.

Iran and Hizbollah hackers have waged several cyber-attacks to the government websites of Bahrain such as Ministry of Interiors, Housing and New Agencies (Grewal, 2011). However, those dealing with security issues of cyber space dealing in Bahrain claims that they got all IT infrastructure and security tools to handle with such activities. This does not lead to the conclusion that online banking system in Bahrain is too secure to be compromised. The recent events are continued proof that the crimes in banking sector are moving away from physical attacks to a harmless more financially profitable tactics of doing it remotely and further the misuse of social media such as Facebook and Twitter has increased the percentage of cyber-crime in Bahrain (Science Alert, 2016).

## **RECOMMENDATIONS**

Based on the data findings and discussion above, this research recommends the followings;

- Banking industry in the Kingdom of Bahrain should move to three factor authentication system by providing additional security devices and key fobs to make sure that all transactions of online banking

services are completely secure. This will alternatively help to boost the confidence of online banking users and will further help in the growth of the business industry.

- The use of secure application software must be introduced or should be increased to increase the layers of online banking security system.
- More sophisticated and robust systems must be developed to monitor the activities of computer fraudsters and hackers to make sure that they do not gain any unauthorized access to the financial information of online banking customers. This will alternatively help the business transactions to be accomplished in secure environment.
- The confidence level of the online banking users must be developed by educating them about the tools and techniques used when dealing with online banking services.
- The awareness about available online threats must be developed among those users who deal with online banking services and the banking industry must take positive initiatives to achieve this objective.
- E-banking customers should be educated more about the importance of changing their online banking passwords to make sure that these passwords can never be predicted by the cyber criminals and other computer fraudsters. Further, all users must take extra care while dealing with online banking services to make sure that their financial data is secure and not accessible to any other individual.
- The banking industry should and must implement more robust and secure system of online banking services to enhance business growth in the Kingdom of Bahrain.

## REFERENCES

- Al-Bawaba, 2016, Bahraini companies no match for thousands of cyber attacks, Published July 22nd, 2012, accessed on 09/02/2016
- CBB, 2016, Central Bank of Bahrain, The Kingdom of Bahrain, [http://www.cbb.gov.bh/iis/register\\_result](http://www.cbb.gov.bh/iis/register_result)
- CRIC, 2005, Trojan Redirector Ups the Ante in Online Banking Attacks, Cyber Criminal Investigation Cell, Crime Branch Criminal Investigation Department Mumbai India, available at <http://cybercellmumbai.gov.in/html/news/trojan-redirector-ups-the-ante-in-online-banking-attacks.html>
- DOPUK, 2013, Bank Distributed Denial of Service (DDoS) Attacks Strikes Could Presage Armageddon, DoS Protection UK, available from <http://www.dos-protection.co.uk/?p=152>
- GoGulf, 2013, Cyber Crime Statistics and Trends, available from <http://www.go-gulf.com/blog/cyber-crime/> accessed at 25 January 2016
- Grewal, SS 2011, Fighting Cybercrime. Gulf Daily News, Bahrain, May 03, 2011, available from <http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=305199>
- IBM, 2015, 2015 Cost of Data Breach Study: Global Analysis, Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute LLC, May 2015
- Kharouni, L 2012, Automating Online Banking Fraud, Automatic Transfer System, The latest Cyber Crime Toolkit Feature, Trend micro incorporated research paper, available from [http://www.trendmicro.com.br/cloud-content/us/pdfs/security-intelligence/white-papers/wp\\_automating\\_online\\_banking\\_fraud.pdf](http://www.trendmicro.com.br/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf)
- Kirsty, 2015, Cyber crime, one of the biggest Middle East Security Threats, posted on January 5, 2015, available from <http://securitymiddleeast.com/2015/01/05/cybercrime-one-biggest-middle-east-security-threats/>, accessed on 25<sup>th</sup> January 2015
- Mishra, P 2014, Cybercrime in the Middle East: A Peep Into Future, Arabian Gazette, Middle East Business News, Dubai News, UAE News, Dubai Events, Dubai Blogs
- NatWest, 2016, Free Rapport Security Software, National West-Minster Bank of United Kingdom, available from <http://personal.natwest.com/global/security-centre/rapport.html>
- OxfordBusinessGroup, 2015, Bahrain's draft legislation on cyber crimes, available from <http://www.oxfordbusinessgroup.com/analysis/new-proposal-cyber-crimes-draft-legislation-addresses-computer-based-criminal-activity>, accessed on 25<sup>th</sup> January 2016
- PandaLabs, 2012, The Quarter at a Glance, Quarterly Report, April-June 2012, available from <http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf>
- RSA, 2016, Online Fraud Resource Centre, Inside the world of fraud and cyber crime, available from <http://www.emc.com/emc-plus/rsa-thought-leadership/online-fraud/index.htm>
- Saunders, M, Lewis, P, and Thornhill, A, 2009. Research Methods for Business Students, 5th Edition, Harlow-Prentice Hall

- Science Alert, 2016, Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status, available from <[http://www.scialert.net/fulltext/?doi=rjbm.2014.139.156&org=10#66603\\_an](http://www.scialert.net/fulltext/?doi=rjbm.2014.139.156&org=10#66603_an)>, accessed on 14 June 2016
- Shaw, A (2013, Bahrain need to tackle the growing problems of cybercrime, Bahrain Institute of Banking Finance (BIBF), Host Cyber Crime and Security available from <<http://www.bizbahrain.com/bahrain-need-to-tackle-the-growing-problem-of-cybercrime/>>, accessed on 12 June 2016
- Sia Partners, 2013, online banking and fraud: A new generation of cybercriminals, Finance and Strategy, The Financial Service Blog of Sia Partners, Available from <<http://en.finance.sia-partners.com/20130228/online-banking-and-fraud-a-new-generation-of-cybercriminals/>>
- SPAMfighter News, 2006, Phishers target bank of Bahrain and Kuwait. SPAMfighter, Denmark.  
<http://www.spamfighter.com/News-6307-Phishers-target-Bank-of-Bahrain-and-Kuwait.htm>.
- Townsend, S 2015, Bahrain probes mobile phone 'identity theft' cases, available from <<http://www.arabianbusiness.com/bahrain-probes-mobile-phone-identity-theft-cases-587395.html#.VrnAK0eLHIU>>
- Unknown, 2006, Denial of Service / Distributed Denial of Service MANAGING DoS ATTACKS, Trusted Information Sharing Network for Critical Infrastructure Protection, Commonwealth of Australia, ISBN 0 642 75362 8, Available from  
<[http://www.dbcde.gov.au/data/assets/pdf\\_file/0011/41312/DoS\\_Report.pdf](http://www.dbcde.gov.au/data/assets/pdf_file/0011/41312/DoS_Report.pdf)>
- Web, P 2013, Online Banking Fraud, Online guards fighting cyber crime, Online banking fraud, process and safety tips available from <[http://www.onlineguards.com/topics\\_onlinebankingfraud.html](http://www.onlineguards.com/topics_onlinebankingfraud.html)>