The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services

Liaqat Ali*, Faisal Ali, Priyanka Surendran, Bindhya Thomas
AMA International University, Bahrain.

* Corresponding author. Email: L.ali@amaiu.edu.bh
Manuscript submitted August 12, 2016; accepted December 23, 2016.
doi: 10.17706/ijeeee.2017.7.1.70-78

Abstract: Cybercrime and information security are always parallel to each other's. Computer fraudsters are always trying to gain unauthorized access to the information of financial and business sectors for fraudulent activities. The customers of online banking always fear for their financial data when dealing with online banking and its services. It is certainly affecting the use of online banking services and its customer's behavior. There is a need to create awareness among online banking customer on how to avoid the available threats. The research in this paper critically analyzes and discusses the effects of cyber threats when dealing with online banking services. It is concluded that by the research that there is a need to increase customer's awareness about available cybercrimes when dealing with online banking and sensitive financial data.

Key words: Cyber crime, online banking, security, financial institutions.

1. Introduction

The rapid growth in cybercrimes 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. Cybercrime is one of the burning issues in today's online banking industry in the world. For appropriate measurements to be implemented, organizations must understand the effects of cybercrimes. 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. The effects of cybercrimes are more than the financial integrity of financial institutions and other organizations. For appropriate measurements to be implemented, organizations must understand the effects of cybercrimes. 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.

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 fingertips but there are issues that must be considered. Understanding the behavior of online banking users is critical when dealing with online banking services. The fear of losing personal information or becoming a victim of online banking services is still there in the modern society of information technology. Security developers are using many tactics to provide secure financial platforms. However, computer fraudsters and criminals are few steps forward.

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.

Online banking has been around since 1981, nearly no cases of fraud have been reported until 2004 [1]. 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 cybercrime is $100 billion [2]. In addition the current estimates value the Middle East cyber security sector at $25 Billion over the next 10 years [3]. Therefore, researchers are continuously warning that financial institutions are the hot spot for the cybercrime and other online fraudulent activities by the cyber criminals. It is therefore important to increase awareness of cyber threats when dealing with online banking services.

Financial institutions and online banking providers certainly understands the sensitivity of cybercrime activities and therefore different legislations have been drafted to be implemented to provide secure environment when dealing with online banking and other financial sectors.

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.

2. Research Importance and Its 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 improve the awareness level of online banking customers. The research paper is 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 scope of the research could be measured through the scope of security and its implementation in online banking sectors. The novelty of this research is based on the comprehensive approach adopted to understand the seriousness of online cyber threats available to online banking industry. The research is unique due to the nature that it details with the effects of cybercrimes on customer's behavior when dealing with online banking services through different digital devices such as personal computers, laptops, iPads and mobiles.

3. Internet and Its Role in Online Banking Services

Internet is one of the fastest growing areas in 21st century which helped in developing technical infrastructure. The rapid growth of the internet applications changed the way people communicate and conduct other businesses in 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 and awareness among online banking users 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 offer 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 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 [4]. 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 [5].

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.

To increase the awareness of available cyber threats among online banking users, it is important that users should understand the available crimes. These cybercrimes are discussed in the further sections of this research.

Identity Theft: Using someone else identity such as name, date of birth, and 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.

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 [6]. 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 [7].

Vishing: Vishsing 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 [8].

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 [9] and there is growing need to develop robust defenses against these sophisticated malware applications targeting online banking services and other financial institutions.

Hacking and Cracking: Through hacking and cracking 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.

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 [10].

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.

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 [11]. *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 [12]*. 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.

Electronic Gadgets and Mobile Phones: 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.

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.

4. Common Security Measures

Online banking users should know common security measures to prevent cyber-attacks and to secure their financial data. The discussed few techniques will be beneficial for all online banking users;

Secure the Device: The security of the device used for online banking access is critical at first stage. These devices include computer systems, mobile and all other gadgets used for the access of online banking.

Protect your Personal Data: Data security is important. Confidential and personal data should not be disclosed to all people. When providing information, one needs to consider the purpose and take extra

measures to avoid any social engineering or other tactics used by computer fraudsters and criminals. Online banking users should understand how to encrypt the data used for financial organizations such as banks and tax returns.

Use Strong Passwords: The use of strong passwords are always recommended for online banking users. Many tools could be used by computer fraudsters to guess or crack the passwords of online banking users. These include Brutus, Rainbow-crack, Wfuzz, Cain and Abel, THC Hydra, OphCrack, Aircrack-NG, Medusa and John the Ripper. It is therefore important to use strong passwords and different user name combinations for different sites and accounts. It is further recommended that passwords should not be written down anywhere. A combinations of different alphabets, number and special characters should be used for a strong password.

Be Secure when Online: The identity of individuals must be protected when dealing online. All social media profiles must be set to private. Security setting of social media accounts should be checked regularly. Private and sensitive information should not be disclosed through the use of social media.

Upgrade your System and Software: It is recommended that online users must upgrade their systems and software to avoid security breaches.

5. Measuring Online Banking Customer's Behaviour

The section of this research deals with the analysis of the survey conducted for this research. The research analyzed the behavior of more than100 online banking users and gauged the effects of cyber threats available to these users. In total, 110 online banking users from education and banking industry participated in the survey of this research. The data was collected from 18 years old and above of online banking customers.

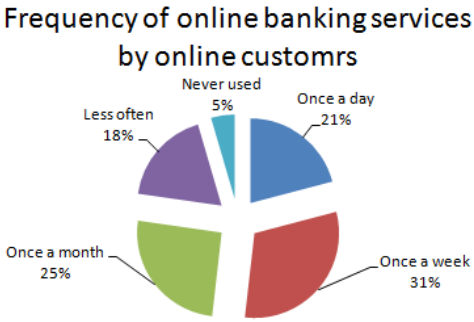

Fig. 1. Frequency measurement.

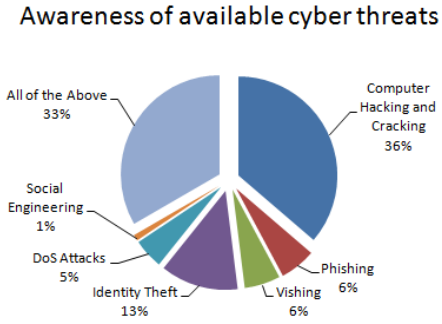

Fig. 2. Awareness measurement.

The above Fig. 1 and its analysis clearyly shows that only 21% of the participants use online banking services every day and 31% use online banking services once a week. The analysis proves that participants

do online banking, except 5%. 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.

The above Fig. 2 analysis proves the level of awareness of the respondents in regard to online banking services and available cyber threats. As shown, 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. On the other hand, it shows that around 70% online banking users got limited awareness about available cybercrimes and threats.

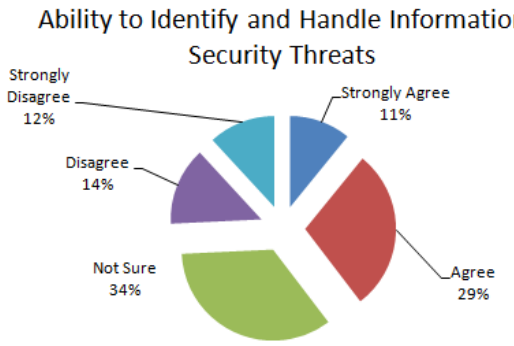

Fig. 3. Ability of handling threats measurement.

The analysis of above Fig. 3 confirmed that only 40% respondents 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 the available threats. 26% respondents as per the above analysis cannot identify such threats and also do not have the ability to handle such threats.

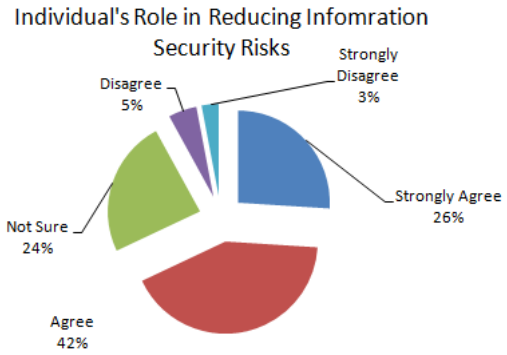

Fig. 4. Individual's role in IS risk measurement.

The analysis of the above Fig. 4 shows that 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.

The analysis of above Fig. 5 proves that 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 since using online banking. The other 8% users are not even aware how to change their passwords of online banking accounts.

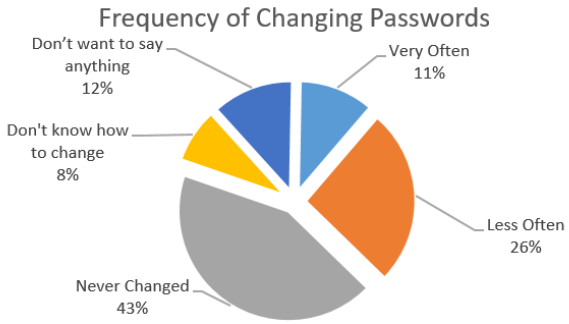

Fig. 5. Frequency of changing passwords measurement.

6. Discussion, Conclusion and Recommendations

The conducted survey of this research based on 110 responses made it possible to draw the conclusion of this research. 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. 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. 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.

The online banking users need to take extra care when dealing with banking 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.

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

- 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.
- Online banking users should use strong passwords and different user name combinations for different sites and accounts.
- E-banking customers should be educated more about the importance of secure online banking environment. Further, all users must take to avoid security threats.

References

[1] Sia, P. (2013). Online banking and fraud: A new generation of cybercriminals, finance and strategy. The

Financial Service Blog of Sia Partners.
[2] GoGolf. (2013). Cyber-crime statistics and trends. Retrieved from the website: <http://www.go-gulf.com/blog/cyber-crime/>
[3] Kirsty. (2015). Cybercrime, one of the biggest Middle East security threats. Retrieved from the website: <http://securitymiddleeast.com/2015/01/05/cybercrime-one-biggest-middle-east-security-threats/>
[4] IBM. (2015). Cost of data breach study: Global analysis, benchmark research sponsored by IBM. Independently Conducted by Ponemon Institute LLC.
[5] Al-Bawaba. (2016). *Bahraini Companies no Match for Thousands of Cyber-Attacks*.
[6] CRIC. (2005). Trojan redirector ups the ante in online banking attacks, cyber criminal investigation cell. Crime Branch Criminal Investigation Department Mumbai India.
[7] RSA. (2016). Online fraud resource centre, inside the world of fraud and cybercrime. Retrieved from the website: http://www.emc.com/emc-plus/rsa-thought-leadership/online-fraud/index.htm
[8] Web. (2013). Online banking fraud, online guards fighting cybercrime, online banking fraud, process and safety tips. Retrieved from the website: http://www.onlineguards.com/topics_onlinebankingfraud.html
[9] PandaLabs. (2012). The Quarter at a Glance, Quarterly Report. Retrieved from the website: http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf
[10] Kharouni, L. (2012). Automating online banking fraud, automatic transfer system, the latest cyber crime toolkit feature, trend micro incorporated research paper. Retrieved from the website: http://www.trendmicro.com.br/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf
[11] DOPUK. (2013). Bank distributed denial of service (DDoS) attacks strikes could presage Armageddon. DoS Protection UK. Retrieved from the website: http://www.dos-protection.co.uk/?p=152
[12] Unknown. (2006). Denial of Service / Distributed Denial of Service MANAGING DoS ATTACKS, Trusted Information Sharing Network for Critical Infrastructure Protection, Commonwealth of Australia.

Liaqat Ali is working as associate professor in AMA International University, the Kingdom of Bahrain. He completed his Phd "E-accessibility of online banking services for visually impaired" in 2008 from United Kingdom. He got a strong research background and has published many papers on cyber crimes and business information systems. He is a UK citizen and a fellow of Higher Education Academy, United Kingdom.

Faisal Ali is assistant professor with AMA International University, the Kingdom of Bahrain. His research is in the field of management sciences and engineering. He published many papers on the subject of management engineering.

Priyanka Surendran is currently working as assistant professor at AMA International University Bahrain. She has obtained her Ph.D from Karpagam University, India. She has more than 10 years' experience in teaching both in India and Bahrain.

Bindhya Thomas works as a lecturer in AMA International University, Bahrain. She had 11 years of experience in teaching and 1.5 years of industry experience. She completed the M.Sc. Computer Science from Bharatiyar University, Coimbatore, India.