A RESEARCH PAPER ON

CYBER CRIME IN BANKING SECTOR OF BANGLADESH

SUBMITTED TO

DEPARTMENT OF LAW

SUBMITTED BY

2016-1-66-006 (Sayeda Fariha Alomgeer)

CYBER CRIME IN BANKING SECTOR OF BANGLADESH

COURSE NAME: SUPERVISED DESSERTATION

COURSE CODE: LAW 406

ID: 2016-1-66-006

DEPARTMENT OF LAW

EAST WEST UNIVERSITY

DECEMBER 2019

TABLE OF CONTENT

Chapter Four

The Mystic Scenario of cyber crime in Banking sector of Bangladesh:

Chapter Five

Laws related to cyber crime in Bangladesh: An Overview

Chapter Six

Findings and Recommendations

Chapter Seven

Reference

DECLARATION

I am Sayeda Fariha Alomgeer hereby declare that the research paper named ‘’CYBER CRIME IN BANKING SECTOR OF BANGLADESH’’ is an original perused under the supervision of Mridul Bepari, Department of Law (EAST WEST UNIVERSITY)

I also declare that this research is free from plagiarism and has not been submitted on the other institution or any other places. The purpose of the inferential criticism is for academic purpose.

DATE: 10 AUGUST 2019

ID NO: 2016-1-66-006

Abstract

This research is based on cybercrime in banking sector of Bangladesh. Here also described the uses of internet and many types of cybercrime which is occurred in online banking sector through internet. The process of cybercrime is described here and the accomplishments of different laws are shown in it. In this thesis described the laws of our country with their defects. It is also focuses the loopholes of our laws. What is the scenario of banking sector in our country also shown in this thesis. However, We have no sufficient laws to deals with cybercrime but it is urgent to enact it also elaborate in this research.

Key Words: Cyber Crime, Online Banking, Computer, Internet

ACKNOWLEGMENT

Firstly, I would like to grateful to Allah who gave me this platform of completing my research properly. Then I would like to give thanks to my honorable supervisor Mridul Bepari for the support in my research paper. Sir was always help me and listen my problems and give advice and also responsible for involving me in this research paper.

I am also grateful to my other respected faculties of Law, EAST WEST UNIVERSITY for their affection and sincerity to complete my inquisition.

And last but not the list, I would like to thank my family members specially my parents for educating me with an unconditional support and a huge encouragement.

Chapter One

Introduction

According to my research topic we can see that my research is related to banking sectors cyber crime occurred in Bangladesh. At present in banking sector Bangladesh has facing many problems regarding cyber crime which is now become an serious issue. It has considered as the serious issue because through online banking system people deposit money in banks, transfers money to another, withdrawn money for different purpose and if banking sectors faces cyber crime then all the people who are dependent on online banking faces many sorts of difficulties. So, I will try my level best to discuss the things how banking sector cyber crime has been occurs, their reasons and also try to focus some laws.

1.1 Objective of research paper

The main object of my research is not to give the solution why the banking sectors cyber crime has been occurred rather I will try to find out the loopholes of the cyber laws and try to give a analytical discussion.

1.2 Research Methodology

This analysis is qualitative in nature. I include the Journals, Laws, Newspapers Articles, and Articles of many scholars. Firstly, I try to find out the problems. The reasons behind cyber crime, different phases and modes of cyber crimes and also how banking sectors cyber crime has been done. Then I try to give the mystic scenario of cyber crime in Bangladesh. Then I find the Acts which are related to such crimes. Then I find the loopholes of our laws and want to give a opinion on it and describe the process to implicate my research.

1.3 Limitation of the Study

Research on the basis of a specific topic is a very huge thing to do. Four months is not enough for research in a topic. Perhaps, I try my best to do a new thing on a short time. But there are no books based on my topic. There are not much journal, Articles to make this research and also its very hard to make public opinion on that topic. We haven’t much law on the basis of my project. Overall there are lots of limitations for this research in this field.

Conclusion

In the second chapter I will try to focus about the Internet and cyber crime in Bangladesh and try to give a brief history of cyber crime in banking, clarification of Internet banking and cyber crime in banking, reasons behind cyber crime, and also different phases and modes of cyber crime.

Chapter Two

Internet and cyber crime in Bangladesh

In this chapter first of all I will give a brief history of internet in banking sectors. Secondly, I will try to cover the clarification of internet and cyber crime of banking sector. In the third segment I will try to find out the main or basic reason behind cyber crime in banking sectors. And lastly, I will try to end up this chapter by clarifying different phases and modes of cyber crime which has been occurred in the modern online banking throughout the world including Bangladesh.

2.1Brief History of internet banking

Basically internet banking has been started in the mid nineties but in 1980's it has been found out properly by the people of this era. They found out that customers attraction on the internet banking and the method of transactions had been very well established. Some banks are dependent on traditional ways of banking on that time. And the others who depend on this banking do not have enough internet based transaction to justify their interest in the internet banking. Some customers turn to internet baking due to the discomfort of traditional banking system. They thought the internet banking system are ensured security and give facilities. For this reason from this time day by day customers interaction in internet banking has been developed.[1]

In the year 1981, first New York City banks have been introduced a test at home- banking. New York city was the first place in the U.S to test out the innovative way of doing business, providing electronic services. In the year 2001, Bank of America found that they have almost 3 million online banking customers. In 2006, online banking had become widespread. About 80% of banks in the U.S were offering internet banking services. After that in 2010, internet banking is growing very fast. At this stage the return of money, transfer of money via text, email, cards have been introduced. Lastly in 2018, Online banking has been developed. Today it is the widespread and very popular among the customers who use the internet banking in their daily basis of life.[2]

In present days, after completing all the stages it has been proved that the banks offer a wider range of online banking services than smaller banks do and also that Internet banks are more profitable than non-Internet banks. Since large and well established banks have already been provided Internet banking services, the growth on the number of banks which will offer Internet banking can be anticipated to come from the smaller banks.[3] Moreover, consumers want to have privacy and to feel confident about the banking institution they are deals with.[4] At present, the status of a bank seems to matter a lot when making the choice among many banks which offer

---

[1]Marcus Peterson, ''A Brief History of Internet Banking'' (2006) https://ezinearticles.com/?A-Brief-History-of-Internet-Banking&id=353450 accessed on 9 November, 2019

[2]Ruth Sarrel, ''History of online Banking: How Internet Banking went Mainstream'' (May 21,2019) https://www.gobankingrates.com/banking/banks/history-online-banking/ accessed on 10 November, 2019

[3] Capco Journal of Financial Transformation, (2001)

[4] Anguelov C. E., Hilgert M.A., and Hogarth J. M.

Internet banking services. Consumers show a preference towards well-established institutions, because now they feel more protected though the modern internet banking system and that their transactions are more secure.[5]

2.2Clarification of Internet Banking/Online Banking/E-Banking

There were perceived risks in online trading,

But the benefit was so high, it was worth it.

With online banking, the risk is greater

And the benefit isn't obvious.

-Jim Bruene[6]

Internet banking/online banking/e-banking is a provision of banking systems and services through electronic devices such as mobile phone computers etc. Electronic banking has been around for quite some time in the form of automatic teller machines (ATMs) and telephone transactions. Recent times, it has been transformed by the internet, that has been facilitated banking transactions for both customers and banks. For customers, the internet offer faster access, which is more convenient for the benefit it provides advantage among the customers.[7]

Basically interest in Internet banking reflects a more general interest in the role of the Internet as a vehicle for commercial activity. Internet banking with other financial services, provides a fertile environment for the development of e-commerce. Banking involves the collection, storage, transfer and processing of information. The Internet makes it an incredibly powerful and efficient tool for handling these information processes.[8]

---

[5]Dispoina Anesti, ''Internet Banking History and Strategies: A case study of U.S And Greek Banks'' (May 20, 2004) https://digitalcommons.csumb.edu/cgi/viewcontent.cgi?article=1369&context=caps_thes accessed on 12 November, 2019

[6]Jim Bruene,(QuoteHD.Com) <http://www.quotehd.com/quotes/jim-bruene-quote-there-were-perceived-risks-in-online-trading-but-the-benefit>

[7]Jayshree Chavan, ''Internet Banking-Benefits and challenges in an emergence economy'' (2013) https://s3.amazonaws.com/academia.edu.documents/37989966/--1371887005-3.Manage-Internet-Jayashree_chavan__1.pdf?response-content-disposition=inline%3B%20filename%3DINTERNET_BANKING-BENEFITS_AND_CHALLENGES.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191112%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191112T114905Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=b32e1570cac0723a81932f87b7f046d5e2874cdd6cf0dd8afbf4b5a2dd312348 Vol, 1 Issue 1, 19-26

[8]John Carlson, Karen Furst, William W. Lang, and Daniel E. Nolle ''Internet Banking: Market Developments and Regulatory Issues (May 2001, Revised) https://pdfs.semanticscholar.org/1660/aa82bfb2310f755f8676dbc9560454a2abeb.pdf

2.3Clarification of Cyber Crime in Banking

It can be defined as computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties
-A.R.Raghavan[9]

Clarification of cyber crime in banking sectors can be defined as digital wrongdoing because it has been done through digital devices or instruments. Digital Wrongdoing can be just expressed as violations which includes the utilization of PC and a network used as a medium source of instrument, target a place of the purpose for wrongdoing. It has expanding all around. Digital Violations can be occurred through digital instruments like Digital harassing, Fakes Email, Phishing and more.[10]

There are number of frauds happened in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. This frauds are executed with the ultimate goal of gaining access to users bank account, steal funds and transfer it to some other bank account. The cyber criminals uses the banking accessories like PIN, password, etc. to access accounts. Most of the times the intention of cybercriminals is to harm the image of the bank and for this they block the bank servers, the clients are unable to access their accounts and damages the financial sectors of that bank.[11]

2.4Reasons behind Cyber attacks

Cyber attack is an attack which has been launched from one or more computers against another computer, multiple computers or networks. The main reason for Cyber attacks can be broke down into two broad categories 1) Attacks when the goal is to disable the target computer or knock it offline 2) Attacks when the goal is to get access to the target computer's data and try to gain privileges on it.[12]

The increasing trend of cyber-attacks has also reached the financial institution. That is why each company, depending on its size, geographical setup, business operating sector, etc should have been developed at its own risk. To maintain companies series of steps which required to implement security controls, covering identification of threats, risks and design and

[9]A.R. Raghavan and Latha Parthiban, ‘’The effect of cybercrime on a Bank’s finances’’ (February, 2014) < https://pdfs.semanticscholar.org/d788/a7cd721b0666ceced932cd7e65111b44cb7f.pdf> Vol 2, pp, 173-178
[10]Harshita Singh Rao, ‘’Cyber Crime in Banking Sector’’ (January 2019) < http://oaji.net/articles/2019/1330-1548742941.pdf> Vol 7, Issue 1
[11] Claessens et al., (2002), Hutchinson & Warren, (2003)
[12]Josh Fruhlinger, ‘’What is cyber attack? Recent Examples show disturbing trends’’ (November 26, 2018) https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

implementation of security controls for addressing these risks when institution failed to do this sorts of things cyber attacks have been occurred.[13]

2.5Different Phases of Cyber Crimes

Cyber Crime can be divided into many phases. The most common phases of cyber crime has been describe below:

Unauthorized Access: Knowingly and intentionally use or access without permission or consent of the owner or possessor wholly or any part of a computer systems. Computer network to commit any cybercrime as defined above is unauthorized access. This is like an criminal trespass.[14]

Cyber Theft or Identity Theft: Identity theft of cyber crime is growing rapidly. Proper care must be taken by the customers to protect their identity and it is also their responsibility to take measures to disallow any data breach. The definition encountered for identity theft is "The use of another individual's personal information without that individual's permission for purposes of committing a crime''.[15]

Cyber Stalking: Cyber stalking is a process of message, sent to unwilling mental torture. A cyber stalker collects all the personal information about the victim such as his name, age, family background, telephone or mobile numbers, workplace etc. Collects all this information from the internet resources such as various profiles the victim may have filled while in opening the chat or e-mail account.[16]

Email Fraud (Spamming): E-mail is an inexpensive and popular device for distributing, fraudulent message to the victims. This process is not only helps to assume someone else identity, but also helps to hide one's own. The purpose of spamming is to trick the person for hacked his information so that the offender can steal his identity and commit crime on the name of that person.[17]

Cyber Defamation: Cyber defamation means any derogatory statement or which intended to injure of person's name or reputation on a website, or sending email containing of defamatory of

---

[13]Andreea Bendovschi, ''Cyber-Attacks- Trends, Patterns and Security Countermeasures'' (April 2015) https://www.sciencedirect.com/science/article/pii/S2212567115010771

[14]Ombo Malumbe, ''Computer hacking and/or unauthorized access: A critical analysis of the legal framework in Kenya'' (2014) https://www.academia.edu/14236657/COMPUTER_HACKING_AND_OR_UNAUTHORIZED_ACCESS_A_CRITICAL_ANALYSIS_OF_THE_LEGAL_FRAMEWORK_IN_KENYA

[15]Atefa Tajpur, Suhani Ibrahim, Mazdak Zamani, ''Identity Theft Methods and Fraud Types'' (October, 2013) https://www.researchgate.net/publication/273259976_Identity_Theft_and_Fraud_Type

[16]Pittaro Michael, ''Cyber Stalking: An analysis of online harassment and Intimidation'' (January, 2017) https://www.researchgate.net/publication/241843583_Cyber_stalking_An_Analysis_of_Online_Harassment_and_Intimidation vol, 1

[17]Hayati, pedram; Potdar, Vidyasagar; Talevski, Alex; Firoozeh, Nazanin; Sarenchech, Saeed; Yeganeh, Elham ''Definition of spam 2.0: New spamming boom'' (May, 2010) https://www.researchgate.net/publication/224185368_Definition_of_spam_20_New_spamming_boom

information's of some other person constitute the offence of cyber defamation. Publication of a statement through the electronic mail, message, chatting without justification of excuse of reputation of which is collected to injure of the another. Charge of any criminal offence, or of fraud dishonesty, dishonest conduct etc. amounts to be defamation.[18]

2.6 Different Modes of Cyber Crime

Computer Network Attack: Cyber Crime Attack is also called **Computer Network Attack.** It is an attack from one computer to another computer using a network. These attacks object is to steal the relevant information. Cyber attacks have been conducted through the Internet. These affect private individuals, companies, organizations and even nations, and also provides a negative impact on the economic and social conditions for the loss of money. These attacks can includes hacked online bank accounts, posting confidential banking information over the Internet.[19]

ATM Card Fraud: ATM card (Automated teller machine) becomes a vulnerable target for exploiting the user ownership and user account as they only rely on the magnetic stripe through a skimming device. Criminals are operating cash machine frauds all over the world. The most common modes to execute the cash point fraud is very small tricky device known as skimmers it simply clone the magnetic stripe of the cash card and enable them to get money. It just put a shell over the ATM card reader so that it looks like a legitimate part of that device. Victims come up and place their cards into this, enter their code and withdraw money and get their card back but they don't realize that the time between their transactions is an illegal device that reads every single piece of data in the card and records it.[20]

Credit card fraud: Credit card fraud can be termed as an unauthorized account activity. Credit Card Fraud is defined as when an individual uses another individual's credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. And the persons using the card has not at all having the connection with the

---

[18]Khairun Nisaa Binti Asari, ''Cyber Defamation: A comparative analysis of the legal position in Malaysia and the United Kingdom (2014) https://www.researchgate.net/profile/Nazli_Ismail_Nawang/publication/266477457_Cyber_Defamation_A_Comparative_Analysis_of_the_Legal_Position_in_Malaysia_and_the_United_Kingdom/links/5b6d2e9c45851546c9f96d85/Cyber-Defamation-A-Comparative-Analysis-of-the-Legal-Position-in-Malaysia-and-the-United-Kingdom.pdf

[19]Dr, Manisha M. More; Meenakshi P. Jadhav; Dr, K. M. Nalawade, (Online Banking and Cyber Attacks: The Current Senario'' (December, 2015) https://www.researchgate.net/profile/Dr_Manisha_More/publication/290325373_Online_Banking_and_Cyber_Attacks_The_Current_Scenario/links/56962a8308ae425c6898fe70/Online-Banking-and-Cyber-Attacks-The-Current-Scenario.pdf Vol 5, Issue 12; accessed on November 13, 2019

[20]Divya Singh; Pratima Kushwaha; Priyanka Choubey; Abishek Vaish* and Utkash Goel, '' A proposed Framework to Prevent Financial Fraud through ATM Card Cloning'' (July 6-8, 2011) http://www.iaeng.org/publication/WCE2011/WCE2011_pp491-494.pdf Vol I

cardholder or the issuer has no intention of making the repayments for the purchase they have been done.[21]

After discussing all this points I want to conclude this chapter. And in the next chapter I will try to give a critical analysis based on cyber crime in banking sector of Bangladesh.

[21]Raghavendra Patidar, Lokesh Sharma, ‘’Credit Card Fraud Detection using Neutral Network’’ (June 2011) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.8231&rep=rep1&type=pdf Vol 1 accessed on November 14, 2019

Chapter Three

Cyber Crime in Banking Sector: A Critical Analysis

In this chapter I try to include what kinds of cyber crime has been occurred in banking sectors. Banking sectors cyber crime, customers and bankers faces different kinds of cyber attacks problem. The cyber crimes which have been related to banking sectors are Hacking, Phishing or Identity Theft, Spyware, Watering Hole, and Credit Card Redirection &Farming. I try to give a small portion of information regarding this cyber attacks.

3.1Hacking

Hacking which means an unauthorized access made by a person for crack down the systems or an attempt to pass the security mechanisms. By hacking the accounts of the customers hackers can get all the confidential information and create a huge amount of loss. Normally hackers hacked bank account by using the computer with the connection of the internet.[22]

3.2Phishing/Identity Theft

Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email. Sometimes, the email has been made to look exactly like a legitimate organization's email. It is a type of fraud that is designed to trick individuals for disclosing confidential, financial information for the purpose of identity theft.[23]

3.3Spyware

Spyware is the way that online banking confidential information have been stolen which is used for fraudulent activities. Spyware works by capturing information either on the computer, while it is transmitted between the computers and websites. Spyware is mainly a software component that monitors client activity, sends the collected data to a remote machine.[24]

---

[22]Robert J. Sciglimpaglia, Jr ''Computer Hacking: A Global Offence'' (September, 1991) https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1020&context=pilr Vol 3, Issue 1

[23]N.P. Singh, PhD ''Online Frauds in Banking With Phishing'' http://www.icommercecentral.com/open-access/online-frauds-in-banks-with-phishing.php?aid=38493 accessed November 14, 2019

[24]Merrill Warkentin; XiN luo; Gary F. Templetion, ''A Framework for Spyware Assessment'' (August 2005) https://www.researchgate.net/profile/Merrill_Warkentin/publication/220423529_A_framework_for_spyware_assessment/links/09e4150f98f118d011000000.pdf Vol 48

3.4Watering Hole

The cyber fraud named ‘’Watering Hole’’ is considered to be a branch which have been arising from phishing attacks. When the victim visits the site with malicious code by the attackers, the information of such victim is then traced by the attacker and causes the attack.[25]

3.5Credit Card Redirection &Farming

In the process of Farming a bank’s URL code is hijacked by the attackers in a manner that when a customer log in to the bank website they are redirected to another website which is fake but looks like an original.[26]

After giving the information of cyber attack that has been faced by the banking sectors I want to conclude this chapter. In chapter Five I will try to cover the scenario of cyber crime in banking sector of Bangladesh.

[25]Ms. Neeta, ‘’ Cyber Crimes in Banking Sector’’ (May 2019) https://www.aiirjournal.com/uploads/Articles/2019/05/3799_08.Ms.Neeta%20&%20Dr.%20V.K.Bakshi.pdf Vol VI, Issue v, accessed November 15, 2019

[26]Sanchi Agarwal, ‘’Cyber Crime in Banking Sector’’ (May 2016) http://www.udgamvigyati.org/admin/images/Cyber%20Crime%20in%20Banking%20Sector-%20Sanchi%20Agrawal.PDF Vol 3

Chapter Four

The Mystic Scenario of Cyber Crime in Banking Sector of Bangladesh

In this chapter I will try to discuss about the mystic scenario of cyber crime by defining some hacking events that happened in the banking sectors of Bangladesh. These are given below:

4.1Sonali Bank Website Hacking

Sonali Bank website had been hacked by a 'Muslim Hacker' on September, 2014. The home page of the Sonali Bank website was found carrying a notice by the hackers. The hacker try to distinguish the network security of Sonali Bank and try to took a control of their website.[27]

The bank has lost Taka 2 crore by the cyber-crooks. Hackers hacked into the bank's security system and transferred the money to an account in Turkey. Fortunately, the bank luckily escaped another hacking attempt as there was no cash in the account from which the hackers tried to steal money.[28]

4.2Six ATM booths had been forced

Bangladesh Bank identified forgery at **Six ATM booths** where the money has been withdrawn form the clients accounts of Eastern Bank Limited by some fraudulent people. The information has been received that the money has been withdrawn from six ATM booths by installing skimming devices and cameras. It was the statement of Eastern Bank after its investigation into the allegation of ATM forgery.[29]

4.3 Bangladesh Bank Hacking

The biggest E-Money laundering that has been occurred in February 2016, named the **Bangladesh biggest bank robbery** in the history of the country. In this hacking the hacker stole more than $80 million from the Bangladesh Bank account via the Federal Reserve Bank of New

---

[27]Staff Correspondent, ''Sonali Bank Website Hacked'' bdnews24.com https://bdnews24.com/bangladesh/2015/12/02/sonali-bank-website-hacked (Bangladesh, Published 2 Dec 2015 11:15 AM; Updated: 2 Dec, 2015 11:44 AM)

[28]Sajjadur Rahman and Rejaul Byron, ''Hackers active'' The Daily Star https://www.thedailystar.net/hackers-active-12573 (Bangladesh, 12:05 AM, February 23, 2014/ Last Modified 01:53 AM, March 08, 2015)

[29]Enamul Hoque Chowdhury(Editor) Published by: Maynal Hossain Chowdhury on behalf of East West Media Group Limited, ''Central Bank identifies forgery at six ATMS'' Daily Sun https://www.daily-sun.com/post/114029/Central-Bank-identifies-forgery-at-six-ATMs (Bangladesh, 14 of February 2016)

York, transferred the accounts to the Philippines, then laundered it through the Philippine casino system.[30]

After discussing all these points I want to conclude this chapter saying that by taking precautionary measures this incidents can be stopped. In the next chapter I will try to give the related laws though I did not found exact laws related to my topic but I try to find out the laws and the loopholes of this laws and try to discuss some case laws also.

[30]Source: AL JAZEERA (Quatari Pay Television News Channel), ‘’Hacked: The Bangladesh Bank Heist’’ < https://www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.html> (Doha, quatar; May 24, 2018)

Chapter Five

Laws Related to Cyber Crime in Bangladesh: An Overview

In this chapter I will try to cover up the laws or Acts which is related to cyber crime in Bangladesh. How this Acts works, and I try to give an opinion regarding the loopholes of this Acts. And lastly I will conclude this chapter through giving the reference of recent cases.

5.1 Digital Security Act, 2018

The **Digital Security Act** was first presented to the parliament in April 2018, along with Bangladesh Minister of Law, Justice and Parliamentary Affairs declare that the Digital Security Act would be revised in consultation with the journalist community.[31]

The **Digital Security Act, 2018** is considered an Act which is coming with an upgraded version of the cyber protection law of the country which recognizes the definition of E-Commerce, E-Transactions etc.

Section 5 states about the constitution of a Digital Security Agency, who shall monitor and supervise the digital contents, communications, mediums including mobile phones to prevent cyber-crime.[32]

Section 13 of the Act illustrates the Power of the DG of (Digital Security Agency), where the DG can order or can banned the communication in extra-ordinary situation to any individual or service provider. The person or service provider got the opportunities to facilitate or monitoring and convert the Computer or source. It illustrates that the cybercrimes in terms of Hacking, violation of privacy in other ways.[33]

In **section 17** illustrates the Punishment for the offenses which is ranging from 14 years Imprisonment and a fine not exceeding taka (1 crore) or both. Another imprisonment or fine provision is 7 years and not exceeding 25 lack taka or both.[34]

---

[31]Rahidul Hasan, ''Digital Security Bill Passed'' The Daily Star < https://www.thedailystar.net/politics/bangladesh-jatiya-sangsad-passes-digital-security-bill-2018-amid-concerns-journalists-1636114> (Bangladesh, 12:00 AM, September 20, 2018/ Last Modified: 07: 30 PM, October 02, 2018)
[32]Digital Security Act 2018, Section (5)
[33]Ibid, S (13)
[34]Ibid, S(17)

Section 21 encompasses that any derogatory comments, remarks, campaign in electronic media made by a person, institution or foreign citizen, against the war of liberation, or father of the Nation Bangabandhu Sheikh Mujibur Rahman, or any issue that has been settled by the Court shall amount to an offense under this Act, it shall be entitled to imprisonment for 10 years and fine not exceeding 1 crore taka or both. Another imprisonment or fine provision is imprisonment for life or fine not exceeding 3 crore or both.[35]

5.2 ICT Act, 2006 & Cyber Tribunal

The parliament of Bangladesh has enacted **Information and Communication Technology Act 2006**, which defines certain activities as crime. The activities which made punishable under the Information and Technology Act of 2006 shall be the cybercrimes for the territory of Bangladesh.[36]

According to **Section 68** of the Information and Communication Technology Act, 2006 for the effective disposal of cases under this Act, Government shall establish one or more **Cyber tribunal**.[37]

Under **Section 69 (1)** the tribunal shall try only the offences under this Act and the Government shall determine the local jurisdiction of the tribunal. In consultation with the Supreme Court, Government shall appoint on Sessions Judge or Additional Sessions Judge as a judge of Cyber Tribunal. Cyber tribunal shall take a case for trial or upon the report of a police officer not below the rank of sub-inspector or complaint made by a controller appointed under this Act or by any other person authorized by the controller.[38]

Under **Section 70 (2)** Cyber tribunal shall apply the provisions of **Criminal Procedure Code** and it shall have the same power, a Sessions Court empowered to apply its original jurisdiction. Public prosecutor shall conduct the case on behalf of the Government.[39]

---

[35]Ibid, S (21)
[36]The Information and Communication Technologies Act, 2006
[37]ICT Act 2006, Section (68)
[38]Ibid, S 69 (1)
[39]Ibid, S 70 (2)

In **Section 73** signifies that the Tribunal shall conclude the trial within six months from the date of framing charge. This period may be extended for another three months. After that Tribunal shall pronounce its judgment.[40]

5.3 Loopholes of the laws

There is a proverb goes "Prevention is better than cure". For prevention of numerous cybercrimes, it is better to initiate advanced technological actions. I will try to find out the practical application of legal remedies and their loopholes which available in Bangladesh for curing the cybercrimes. First I want to mention that in **Banking Companies Act, 1991** there is no provision of online banking for the remedy of cyber crime that is the biggest loopholes of the laws. Besides, we have noticed that in the **ICT Act, 2006** it is hardly being tried to locate all the probable grounds of cybercrime which is frequently occur at present days and which might occur in future days as well. However, as per the provisions of the ICT Act a good number of other procedural and structural provisions, but the judges and the lawyers are the experts of laws, not of internet technology.[41]

So, I think that the judges as well as the lawyers should be trained and made expert in technological knowledge for prevent technological disputes. As I think that the judges have the opportunity to be assisted by the ICT expert. But the reality of our country is so far as no initiative has been taken by the government to train up the judges for acquiring the minimum technological knowledge which is requirement for ensuring justice..

Under **Section 82 (2), (3)** of the **ICT Act, 2006** defines that a police officer not below the rank of a Sub-Inspector can be the IO (Investigation Officer) regarding the cybercrimes.[42]

Here we can see that like the judges, police officers have no opportunity to gather the technological knowledge due to the lack of proper initiatives. It may create a bad impact to ensure justice.

---

[40]Ibid, S (73)
[41]Ashiquddin Mohammad Maruf; Md Rabiul Islam; Bulbul Ahamed, ''Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies'' (2010) https://www.banglajol.info/index.php/NUJL/article/view/18529 Vol 1, accessed November 17, 2019
[42]ICT Act 2006, Section 82 (2),(3)

The government bears the responsibility not only of forming the cyber tribunals but also for preparing terms and conditions of the service of the judges of those proposed tribunals under **Section 82 (4)**.[43] Unfortunately there is not a single rule which has been enacted to form a project or a proposal which have been taken or passed so far by the state.

Circumstances defines that inadequate execution of the ICT Act, 2006 is one of the causes for the increasing cybercrimes. The solution of these issues demands that the state should take precautionary steps and also provides monetary help. States effective steps could able to reduce cyber crime.

5.4 Recent Cases

Case One: An information has been concerned about the Dutch Bangla Bank (ATMs), theft emerged as investigators discovered that it was nine ATMs of the bank, that had been hacked by an international hackers group. After that the Criminal Investigation Department (CID) of police filed a money laundering case along with Badda (Dhaka) Police Station. Before a case was filed by the bank authorities under the Digital Security Act, 2018. It was found that almost Taka 16 lakh was stolen from a total of nine of the bank's ATMs in different areas. After scrutinizing the CCTV footages of the ATMs, the investigators suspected that around 12 to 15 Ukrainians were there who are believed to be the members of an international hackers group. The suspects landed in Dhaka together and stole money from an ATM booth in middle Badda. Taka 4.5 lakh was stolen from the Badda ATM booth. At the time of theft, one of the hackers was detained while he was trying to steal money from the bank's ATM at Khilgaon, (Dhaka). During attempted to the theft, two of the foreigners went to the booth wearing masks and caps. The security guard and local people were able to catch one of them and handed him over to the police. One member of the gang is still missing. Dutch Bangla Bank Ltd authorities also filed a case against the Ukrainians and other unnamed people along with Khilgaon Police Station under the Digital Security Act, 2018.[44]

[43]ICT Act 2006, Section 82 (4)
[44]Staff Correspondent, ''9 DBBL ATMs Victims of int'l fraud gang'' The Daily Star < https://www.thedailystar.net/frontpage/9-dutch-bangla-bank-atms-victim-of-international-fraud-gang-1755148> (Bangladesh, 12:00 AM, June 11, 2019/ Last Modified: 03:54 AM, June 11, 2019

Case Two: In February, 2016 hackers stole $101 million from the Bangladesh Bank account. It is considered as the biggest E-money laundering in the history of banking sector in Bangladesh. Hackers stole $101 million from the BB's account via the Federal Reserve Bank in New York. On the amount $81 million was transferred to four accounts to RCBC (Rizal Commercial banking corporation) in Manila and another $20 million to a bank in Srilanka. But the $20 million which was transferred in Srilanka was failed because of a spelling error of the hacker.[45]

This attack resulted in the theft $101 million, of which $81 million is still missing. Bangladesh Bank has blamed North Korean hackers for helping to steal the money, including the Philippines. The cash has been transferred to the casinos of Philippines. Such large amount of theft from national reserve astonished the people of Bangladesh. Different investigations are being carried by various enquiry commissions like, Bangladesh Bank appointed committee, CID officials of Bangladesh etc.[46]

After discussing all the things I want to conclude this chapter. But, before Conclude this chapter I want to say that in the last chapter that means in Chapter Seven I will try to focus on some points which can be related to my opinion, and try to give recommendation regarding my research topic.

[45]Mehedi Hasan, ''Report in Bangladesh Bank heist case on May 21'' Dhaka Tribune https://www.dhakatribune.com/business/banks/2019/04/17/report-in-bangladesh-bank-heist-case-on-may-21 (Bangladesh, Published at 01:25 pm April 17th, 2019)

[46]Mathew J. Schwartz, ''Bangladesh Bank sues to Recover Funds After Cyber Heist'' (February 4, 2019) < https://www.bankinfosecurity.com/after-cyber-heist-bangladesh-bank-sues-to-recover-funds-a-11993> accessed on November 18, 2019

Chapter Six

Findings And Recommendations

In this chapter I will discuss about the things that I have been found regarding my research. I will try to conclude this chapter by giving some recommendations in different perspectives.

6.1 Findings of the Study

On the basis of my research I found some problems which I want to discuss,

First of all, our **Information and Communication Technology Act, 2006** is not sufficient for dealing with this cybercrime occurred in banking sector. This Act only dealing with the cybercrime, but it is not clear and sufficient. However, Punishment is also not appropriate for that sought of crime, mentioned in Information and Communication Technology Act, 2006. Also in this law there is no mentioned of cybercrimes at all, it is only the law which describes all types of communication system.

Secondly, to protect the cybercrime government makes the **Digital Security Act 2018**, which I have noticed that this Act is also almost same as Information and Communication Technology Act, 2006. There is no any basic changes has been found to control cybercrime. It only describes what is lawful access and what is unlawful access. It is not clear and also very controversial. There has no exact section which is related to cyber crime in banking sector.

6.2 Recommendations

It is very important that the Government should enact the proper law regarding cyber crime in banking sector. On the basis of this research I want to recommend some legal and technical solutions;

According to the **Legal Perspective** there should be forensic bureau which is competent to IT security for investigations/collection of digital cybercrimes evidences. Punishments should be enforced. Sufficient training, awareness to citizens, organizations, and the Government and public in general have to focus on forensic evidences. The maintenance or software installation on our computer we have to consult with our service provider or a certified computer technician.

According to the **Technical Perspective** there should be a use of updated antivirus. Train employees not to open attachments unless they are expecting them necessary. If Bluetooth is not required for mobile devices, it should be turned off. If we require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. Do not accept applications that are unsigned or sent from unknown. Use protection for the most sensitive files such as tax returns or financial records, make regular back-ups of all our important data, and store it in another location. Wi-Fi (wireless fidelity) networks at home are vulnerable to intrusion if they are not properly secured. Default settings have to be modified. Try to avoid conducting financial or corporate transactions on these networks.[47]

After giving all the descriptions I want to conclude this chapter. And I have almost finished my research and at the end try to give an overview regarding the whole topic and finished my work properly.

[47]Kamrul Faisal, ‘’Recent Trend And Issues of Cyber Crime In Bangladesh: An Analytical Study’’ (July 2016) < https://www.researchgate.net/publication/329178520_RECENT_TREND_AND_ISSUES_OF_CYBER_CRIME_IN_BANGLADESH_AN_ANALYTICAL_STUDY>

Chapter Seven

Conclusions

My research is on the basis of cybercrime in banking sector of Bangladesh. In this research I want to suggest to our government to enact the proper cyber law because our laws contains many loopholes, making an individual for an independent body to investigate in that matter only. Nowadays there have a new communication system, in this system we can see a dramatic change in the digital technology system. But the security system for using internet is not so strong. In this research I found that banking sector is under a serious cyber threat. Bangladesh is a digital developing country and the number of internet users increase rapidly, but we do not have anybody to control them. For that reason, we can see the problems as like the stealing money from the bank, through mobile or computer. All types of crime also held by using internet, but we do not have a proper body to handle it. Cyber criminals are using emails, hacking of websites, defamation of private information of respected and popular individuals of the country are some of the examples of cybercrime in banking sectors of Bangladesh.

Lastly, it is very important to say that without proper education about the internet, we cannot make a safe house of internet. To make a secure online banking in this country it is very important to make a strong law on the basis of situation. It is very important to think that all cybercrimes are like as criminal crimes. And we try to protect our country as soon as possible.

Reference

Bibliography

- Marcus Peterson: A Brief History of Internet Banking (2006)
- Ruth Sarrel: History of online Banking: How Internet Banking went Mainstream (May 21, 2019)
- Capco Journal of Financial Transformation, (2001)
- Anguelov C. E., Hilgert M.A., and Hogarth J. M.
- Dispoina Anesti: Internet Banking History and Strategies: A case study of U.S And Greek Banks (May 20, 2004)
- Jayshree Chavan: Internet Banking-Benefits and challenges in an emergence economy (2013) Vol 1 Issue 1 (19-26)
- John Carlson, Karen Furst, William W. Lang, and Daniel E. Nolle: Internet Banking: Market Developments and Regulatory Issues (May 2001, Revised)
- A.R. Raghavan and Latha Parthiban: The effect of cybercrime on a Bank's finances (February, 2014) Vol 2, Page (173-178)
- Harshita Singh Rao: Cyber Crime in Banking Sector (January 2019) Vol 7, Issue 1
- Josh Fruhlinger: What is cyber attack? Recent Examples show disturbing trends (November 26, 2018)
- Andreea Bendovschi: Cyber-Attacks- Trends, Patterns and Security Countermeasures (April 2015)
- Ombo Malumbe: Computer hacking and/or unauthorized access: A critical analysis of the legal framework in Kenya (2014)
- Atefa Tajpur, Suhani Ibrahim Mazdak Zamani: Identity Theft Methods and Fraud Types (October, 2013)
- Pittaro Michael: Cyber Stalking: An analysis of online harassment and Intimidation (January, 2017) Vol, 1
- Hayati, pedram; Potdar, Vidyasagar; Talevski, Alex; Firoozeh, Nazanin; Sarenchech, Saeed; Yeganeh, Elham: Definition of spam 2.0: New spamming boom (May, 2010)
- Khairun Nisaa Binti Asari: Cyber Defamation: A comparative analysis of the legal position in Malaysia and the United Kingdom (2014)

- Dr, Manisha M. More; Meenakshi P. Jadhav; Dr, K. M. Nalawade: (Online Banking and Cyber Attacks: The Current Senario (December, 2015) Vol 5, Issue 12
- Divya Singh; Pratima Kushwaha; Priyanka Choubey; Abishek Vaish* and Utkash Goel: A proposed Framework to Prevent Financial Fraud through ATM Card Cloning (July 6-8, 2011) Vol I
- Raghavendra Patidar, Lokesh Sharma: Credit Card Fraud Detection using Neutral Network (June 2011) Vol 1
- Robert J. Sciglimpaglia, Jr ''Computer Hacking: A Global Offence'' (September, 1991) Vol 3, Issue 1
- N.P. Singh, PhD: Online Frauds in Banking With Phishing
- Merrill Warkentin; XiN luo; Gary F. Templetion: A Framework for Spyware Assessment (August 2005) Vol 48
- Ms. Neeta: Cyber Crimes in Banking Sector (May 2019) Vol VI, Issue v
- Sanchi Agarwal: Cyber Crime in Banking Sector (May 2016) Vol 3
- Ashiquddin Mohammad Maruf; Md Rabiul Islam; Bulbul Ahamed: Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies (2010) Vol 1
- Mathew J. Schwartz: Bangladesh Bank sues to Recover Funds After Cyber Heist (February 4, 2019)
- Kamrul Faisal: Recent Trend And Issues of Cyber Crime In Bangladesh: An Analytical Study (July 2016)

Newspaper Report

- Staff Correspondent, ‘’Sonali Bank Website Hacked’’ (Bangladesh, Published 2 Dec 2015 11:15 AM; Updated: 2 Dec, 2015 11:44 AM) bdnews24.com

- Sajjadur Rahman and Rejaul Byron, ‘’Hackers active’’ (Bangladesh, 12:05 AM, February 23, 2014/ Last Modified 01:53 AM, March 08, 2015) The Daily Star

- Staff Correspondent, ‘’9 DBBL ATMs Victims of int’l fraud gang’’ (Bangladesh, 12:00 AM, June 11, 2019/ Last Modified: 03:54 AM, June 11, 2019 The Daily Star

- Mehedi Hasan, ‘’Report in Bangladesh Bank heist case on May 21’’ (Bangladesh, Published at 01:25 pm April 17th, 2019) Dhaka Tribune

- Enamul Hoque Chowdhury(Editor) Published by: Maynal Hossain Chowdhury on behalf of East West Media Group Limited, ‘’Central Bank identifies forgery at six ATMS’’ (Bangladesh, 14 of February 2016) Daily Sun

- Source: AL JAZEERA (Quatari Pay Television News Channel), ‘’Hacked: The Bangladesh Bank Heist’’ (Doha, quatar; May 24, 2018)

- Rahidul Hasan: Digital Security Bill Passed’’ (Bangladesh, 12:00 AM, September 20, 2018/ Last Modified: 07: 30 PM, October 02, 2018) The Daily Star

Website Visited

1. https://ezinearticles.com/?A-Brief-History-of-Internet-Banking&id=353450

2.https://www.ukessays.com/essays/marketing/the-history-and-background-of-internet-banking-marketing-essay.php#citethis

3. https://www.gobankingrates.com/banking/banks/history-online-banking/

4. https://digitalcommons.csumb.edu/cgi/viewcontent.cgi?article=1369&context=caps_thes

5.https://s3.amazonaws.com/academia.edu.documents/37989966/--1371887005-3.Manage-Internet-Jayashree_chavan__1.pdf?response-content-disposition=inline%3B%20filename%3DINTERNET_BANKING-BENEFITS_AND_CHALLENGES.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191112%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191112T114905Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=b32e1570cac0723a81932f87b7f046d5e2874cdd6cf0dd8afbf4b5a2dd312348

6.https://www.researchgate.net/profile/Ghazi_Al-Weshah/publication/264824344_The_role_of_internet_banking_in_continuous_improvement_areas_Quantitative_evidence_from_Jordanian_banks/links/54f4ffd30cf2ba61506449fe.pdf

7.https://pdfs.semanticscholar.org/1660/aa82bfb2310f755f8676dbc9560454a2abeb.pdf

8.http://oaji.net/articles/2019/1330-1548742941.pdf

9.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.429.2011&rep=rep1&type=pdf

10.https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

11.https://www.sciencedirect.com/science/article/pii/S2212567115010771

12.https://s3.amazonaws.com/academia.edu.documents/39598215/Cyberpower-I-Chap-13.pdf?response-content-disposition=inline%3B%20filename%3DCyberpower_I_Chap_13.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191112%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191112T135435Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=a8de8dfaedbcc64bf06a371950a59e336db6d2f71821a46fbf10547381a3254b

13.https://www.academia.edu/14236657/COMPUTER_HACKING_AND_OR_UNAUTHORIZED_ACCESS_A_CRITICAL_ANALYSIS_OF_THE_LEGAL_FRAMEWORK_IN_KENYA

14.https://www.researchgate.net/publication/273259976_Identity_Theft_and_Fraud_Type

15.https://www.researchgate.net/publication/241843583_Cyber_stalking_An_Analysis_of_Online_Harassment_and_Intimidation

16.https://www.researchgate.net/publication/224185368_Definition_of_spam_20_New_spamming_boom

17.https://www.researchgate.net/profile/Lalitha_Bhaskari/publication/49597043_A_Comprehensive_Analysis_of_Spoofing/links/58d36efa458515e6d900cc0a/A-Comprehensive-Analysis-of-Spoofing.pdf

18.https://www.researchgate.net/profile/Nazli_Ismail_Nawang/publication/266477457_Cyber_Defamation_A_Comparative_Analysis_of_the_Legal_Position_in_Malaysia_and_the_United_Kingdom/links/5b6d2e9c45851546c9f96d85/Cyber-Defamation-A-Comparative-Analysis-of-the-Legal-Position-in-Malaysia-and-the-United-Kingdom.pdf

19.https://www.researchgate.net/profile/Dr_Manisha_More/publication/290325373_Online_Banking_and_Cyber_Attacks_The_Current_Scenario/links/56962a8308ae425c6898fe70/Online-Banking-and-Cyber-Attacks-The-Current-Scenario.pdf

20.http://www.iaeng.org/publication/WCE2011/WCE2011_pp491-494.pdf

21.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.671.902&rep=rep1&type=pdf

22.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.8231&rep=rep1&type=pdf

23.https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1020&context=pilr

24.https://popcenter.asu.edu/sites/default/files/problems/credit_card_fraud/PDFs/Bhatla.pdf

25.http://www.icommercecentral.com/open-access/online-frauds-in-banks-with-phishing.php?aid=38493

26.https://www.researchgate.net/profile/Merrill_Warkentin/publication/220423529_A_framework_for_spyware_assessment/links/09e4150f98f118d011000000.pdf

27.https://www.aiirjournal.com/uploads/Articles/2019/05/3799_08.Ms.Neeta%20&%20Dr.%20V.K.Bakshi.pdf

28.http://www.udgamvigyati.org/admin/images/Cyber%20Crime%20in%20Banking%20Sector-%20Sanchi%20Agrawal.PDF

29.https://bdnews24.com/bangladesh/2015/12/02/sonali-bank-website-hacked

30.https://www.thedailystar.net/hackers-active-12573

31.https://www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.html

32.https://www.daily-sun.com/post/114029/Central-Bank-identifies-forgery-at-six-ATMs

33.https://www.thedailystar.net/politics/bangladesh-jatiya-sangsad-passes-digital-security-bill-2018-amid-concerns-journalists-1636114

34.https://www.banglajol.info/index.php/NUJL/article/view/18529

35.http://www.quotehd.com/quotes/jim-bruene-quote-there-were-perceived-risks-in-online-trading-but-the-benefit

36.https://www.thedailystar.net/frontpage/9-dutch-bangla-bank-atms-victim-of-international-fraud-gang-1755148

37.https://www.dhakatribune.com/business/banks/2019/04/17/report-in-bangladesh-bank-heist-case-on-may-21

38.https://www.researchgate.net/publication/329178520_RECENT_TREND_AND_ISSUES_OF_CYBER_CRIME_IN_BANGLADESH_AN_ANALYTICAL_STUDY

39.https://www.scribd.com/document/292349548/Cyber-Crimes-in-Banking-Sector

40.https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf