International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 10-05-2024, Accepted: 31-05-2024, Published: 25-06-2024
Volume 10, Issue 3, 2024, Page No. 214-219

Emerging cyber security threats in banking sector; Loopholes and solutions in the eye of law

Mehenaj Jerin Mohona
Lecturer, Department of Law and Justice, Bangladesh Army University of Engineering & Technology, Qadirabad Cantonment, Natore, Bangladesh

Abstract
People are living in an era of Internet. Through internet they can easily do many of thrie everyday things which were hard to do previously. Banking system is becoming internet based now-a-days but its not a new concept. E-banking system has made our banking more easier. But it is not free from threats of criminals; which is called cyber crimes. This study contains discussion about the history of e-banking. Here also discussed about the emerging security threats in e-banking sector and loopholes in the existing laws and about what Bangladesh should do to prevent such crimes. The objective of this study is to unearth the development of e-banking in Bangladeshi banking sector and find out existing cyber security challenges faced in e-banking sector. This study ascertain the need for further government action on regulating emerging cyber threats in e-banking sector, find out legal remedies & to analysis the application of relevant laws in Bangladesh in this specific arena.

Keywords: Internet banking, cyber threats, criminals, conventions, statutes, software, security

Introduction

"Electronic Banking" or "E-Banking" is a fuzzy term; it can be defined in several ways. In a simple way, this may mean providing information or services by a bank to its customers, via a computer, a television, or a mobile phone. The definition of e-banking, a contraction of electronic banking, varies greatly from one author to another. Authors sometimes refer to distinct aspects, sometimes to the same thing, or overlap partly [1], below some definitions are given:

- **Electronic banking:** refers to the provision of retail and small value banking products and services through electronic channels. Such products and services can include deposit-taking, lending, account management, the provision of financial advice, electronic bill payment, and the provision of other electronic payment products and services such as electronic money [2].

- **Electronic banking or e-banking:** form of banking where an account is maintained via the Internet rather than, or as well as, at a bank branch [3].

- **E-banking:** web-banking, pc-banking, net-banking, home-banking, etc. Different terms refer to the "Electronic Banking". Thanks to the web, you have the possibility to manage your account from your home [4].

In 1967, the Barclays Bank of UK established Cash Dispenser at first. The working procedure of this machine was quite different from the machine used now. In those days, there were no magnetic cards. Bank gave paper voucher to its clients and when the clients would insert these vouchers in the machine 10 pounds would come out. Later on, plastic cards were used. Within one year of the establishment of cash dispenser by Barclays bank, France, Sweden and Switzerland started "National Cash Dispenser Network". In 1969, Japan and USA started the use of these types of machines produced by them. The machines of that time were in off-line; there was no connection with the computer. Machines of the second era: In 1972, Lloyd's Bank of UK established the very first on-line "Cash Point" machine. They supplied plastic cards to their clients. There were magnetic stripes on those cards. As a result, the client's accounts or the client could be identified. In this on-line system, every machine was connected with the central computer [5]. The Internet explosion in the late-1990s made people more comfortable with making transactions over the web. Despite the dot-com crash, e-banking grew alongside the Internet. While financial institutions took steps to implement e-banking services in the mid-1990s, many consumers were hesitant to conduct monetary transactions over the web. It took widespread adoption of electronic commerce, based on trailblazing companies such as America Online, Amazon.com and eBay, to make the idea of paying for items online widespread. By 2000, 80 percent of U.S. banks offered e-banking. Customer use grew slowly. However, a significant cultural change took place after the Y2K scare ended. In October 2001, Bank of America customers executed a record 3.1 million electronic bill payments, totaling more than $1 billion. In 2009, a report by Gartner Group estimated that 47 percent of U.S. adults and 30 percent in the United Kingdom bank online [6]. There have been several major challenges and issues faced to the e-banking growth and the e-business in general. One major obstacle addressed most is the security concern [7, 8]. E-banking services have been available in Bangladesh since 2001. As of 2007, 29 out of 48 banks have offered online financial services [9]. In Bangladesh, research has been done on electronic commerce issues [10] (Azam, 2007), computer usage [11] (Azam, 2005), Internet usage [12] (Awal, 2004), telephone [13] (Khan, 2001) and electronic banking [14] (Bakta *et al*., 2007).

Multinational banks are operating for long besides our nationalized, private and specialized banks in Bangladesh. However, much of the resulting research has concentrated on providing evidence of the association between consumers' usage patterns of ATMs and their demographic profiles [15, 16] and, more recently, consumer psychographic profiles [17] (Stevens *et al*., 1986). Besides, the banking services of nationalized, private, and multinationals are different by quality of their services. Multinational banks

are offering better services than others. Moreover, waiting to introduce intensive e banking of the multinational banks in Bangladesh. Customer always demands better services, security, and round the clock banking. Multinational banks are considering customers needs and demand in the first line of preference. Moreover, trying to offer and introduce the demanded services by the Bank and changing their offering based on the needs of present and potential customers. Only a few studies regardless of research context have been conducted which focus on the attributes of innovations, as perceived by potential users [18]. The reason for the lack of complete adoption of e-banking in developing countries like Bangladesh is an important research that will be addressed by this paper. In other words, despite this growth of IT Worldwide, Bangladeshi banks continue to conduct most of their banking transactions using traditional methods. Understanding the reasons for the lack of such technological innovation in developing countries such as Bangladesh will develop a fruitful research.

Methodology of the study

This study is primarily based on secondary data. The data and information have collected from government reports, website, newspapers, online blogs, Journals, and Research paper, etc. There conducted a small survey to get the primary data to learn about the upcoming cyber threats in e-banking. Dhaka and Chittagong are two major cities that have seen significant development of e-banking. This paper analyzes those data that present in reports. Here also discussed the various factors that have a substantial impact on E-banking development in Bangladesh. The aim is to help the legislators that want to protects e-banking in Bangladesh. Provide them with a better understanding of Bangladesh's e-banking development, and about the upcoming cyber threats. The understanding of types of threats and loopholes of regulatory framework is enormously crucial for ensuring appropriate strategy for protecting e-banking in Bangladesh.

Present E-Banking services in Bangladesh

E-banking might be implemented in the three main categories of e-commerce business models: Business-to-Consumer (B2C) (e.g., a customer is withdrawing cash from her bank), Business-to-Business (B2B) (e.g., funds being transferred from one bank to another) and Consumer-to-Consumer (B2C) (e.g., funds being transferred between two customers' account). In this paper, we mainly focus four types of e-banking services from the B2C business model category: ATM-based banking, tele-banking, SMS-based banking and Internet banking. At present, several private commercial banks (PCBs) and foreign commercial banks (FCBs) in Bangladesh offer limited services of tele banking, internet banking, and online banking facilities working within the branches of individual bank in a closed network environment. The FCBs have played the pioneering role with adoption of modern technology in retail banking during the early 1990s whereas the state-owned commercial banks (SCBs) and PCBs came forward with such services in a limited scale during the late 1990s.

- **ATM-based banking**

ATM is a virtual teller point of a bank that performs most of the tasks of a teller, including cash deposit/withdraw, balance inquiry, show statement, etc. In Bangladesh, some multinational private banks incepted the ATM booth in Dhaka in 1992. In Bangladesh, for six years from 2004 to 2010, the indicator number of ATMs (per 100,000 adults) increased from 0.14 to 1.93, which implies that the number of ATMs is growing significantly [19].

- **PC banking:** PC banking refers to use of personal computer in banking activities while under PC home banking customers use their personal computers at home or locations outside bank branches to access accounts for transactions by subscribing to and dialing into the banks' Internet proprietary software system using password. Basically, PC banking may be categorized into two types such as online banking and Internet banking.

a. Online banking: At present, 29 scheduled banks offer any branch banking facilities through their respective bank online network that provides facilities like transaction through any branch under the respective bank online network; payment against pay order or pay order encashment, demand draft encashment, opening or redemption of FDR from any branch of the same bank; remote fund transfer, cash withdrawal, cash deposit, account statement, clearing and balance enquiry within branches of the same bank; and L/C opening, loan repayment facility to and from any branch of respective bank under its own online network.

b. Internet banking: German banks have been offering the Internet banking since the mid-nineties, although the only product they were offering at the time was information. Only 7 out of 48 banks are providing some banking services via internet that include account balance enquiry, fund transfer among accounts of the same customer, opening or modifying term deposit account, cheque book or pay order request, exchange rate or interest rate enquiry, bills payment, account summary, account details, account activity, standing instructions, loan repayment, loan information, statement request, cheque status enquiry, stop payment cheque, refill prepaid card, password change, L/C application, bank guarantee application, lost card (debit/credit) reporting, pay credit card dues, view credit card statement, or check balance.

- **Tele-Banking**

To access tele-banking services, customers have to dial a particular telephone number provided by the bank. A customer's identity is verified by checking a PIN or security questions. The full service might be automated although an operator might be reached sometimes. A number of banking services could be realized through tele-banking including detailed account information, balance inquiry, information about products or services, ATM card activation, cheque book related services, bill payment, credit card services, etc.

- **Mobile Banking**

SMS banking is a type of mobile banking, a technology enabled service offering from banks to its customers, permitting them to operate selected banking services over their mobile phones using SMS messaging. SMS banking services are operated using both push and pull messages. Push messages are those that the bank chooses to send out to a customer's mobile phone, without the customer initiating a request for the information. Typically push messages could

be either Mobile marketing messages or messages alerting an event which happens in the customer's bank account, such as a large withdrawal of funds from the ATM or a large payment using the customer's credit card, etc.

Cyber Security Threats in E-banking Sector in Bangladesh

Definition of Cyber Security Threat

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors. Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties [20].

Cyber threats come from numerous threat actors including

- Hostile nation-states
- Terrorist groups
- Corporate spies and organized crime organizations
- Hacktivists
- Disgruntled insiders
- Hackers

Types of Cyber Security Threats in E-Banking Sector in Bangladesh

a. Identity theft

Every year it is estimated that the banking sector suffers a loss of over $ 10 million through identity theft. According to the research by Javelin Strategy and Research, over 15 million Customer in the United States of America have fallen victim to this kind of fraud. Identity theft is the use of persons and credit information without his or her consent to borrow money and conduct a purchase. When a data breach occurs, the data of the customers are either sold or bought in dark web by other cybercriminals to use in other violations of the customer account or financial sector.

b. Malware

Malware is also known as malicious code or malicious software. Malware is a program inserted into a system to compromise the confidentiality, integrity, or availability of data. It is done secretly and can affect your data, applications, or operating system. Malware has become one of the most significant external threat to systems. Malware can cause widespread damage and disruption, and requires huge efforts within most organizations. Spyware, a malware intended to violate privacy, has also become a major concern to organizations. Although privacy-violating malware has been in use for many years, it has become much more common recently. Spyware invades many systems to track personal activities and conduct financial fraud. Organizations also face similar threats from several forms of non-malware threats. These forms of cyber threats are often associated with malware. A more common form is phishing. Phishing involves tricking individuals into revealing sensitive or personal information.

c. Ransomware

Ransomware prevents or limits users from accessing their system via malware. Ransomware asks you to pay a ransom using online payment methods to regain access to your system or data. Online payment methods usually include virtual currencies such as bitcoins. Ransomware is one of the most widely used methods of attacks. Ransomware enters computer networks and encrypts files using public-key encryption. Unlike other malware, this encryption key stays on the cyber criminal's server. Cyber criminals will request ransom for this private key. Cyber criminals are using encryption as a weapon to hold the data hostage. Ransomware is hard to detect before it's too late, and ransomware techniques continue to evolve. Because of this, your institution should focus on prevention efforts. Prevention efforts include training for employees and strong information security controls. The DOB recommends developing strong business continuity plans and incident response plans. Plan development may help in the event of a ransomware attack.

d. Spam & Phishing

Spam includes unwanted, unsolicited, or undesirable messages and emails. Phishing is a form of social engineering, including attempts to get sensitive information. Phishing attempts will appear to be from a trustworthy person or business. Cyber criminals pretend to be an official representative sending you an email or message with a warning related to your account information. The message will often ask for a response by following a link to a fake website or email address where you will provide confidential information. The format of the message will typically appear legitimate using proper logos and names. Any information entered into the fake link goes to the cyber criminal.

e. Data theft and data manipulation stems from new vulnerabilities and cybercriminal behaviors

While threat actors continue to target data their motivations often go beyond theft to include destruction and disruption. A new wave of cyberattacks sees data no longer simply being copied, but being destroyed—or changed—breeding distrust. In late 2019, security researchers disclosed a Microsoft Azure vulnerability referred to as Black Direct. If not remediated, threat actors could exploit this vulnerability to steal sensitive data, compromise production servers, manipulate data, or even encrypt all of a victim organization's data (ransomware). This vulnerability disclosure came as financial institutions and regulators were scrutinizing cloud security vulnerabilities and related cyber threats following the large scale data theft from a major United States financial institution.

f. Theft of money

Cyberattacks may gain access to credit card numbers or bank accounts to steal money. Internet banking has made financial transactions more convenient and accessible for millions of people worldwide. However, this convenience of online banking comes with the risk of Internet banking fraud. Cybercriminals are constantly devising new methods to defraud unsuspecting individuals and organisations of their hard-earned money. People need to learn how they can be duped to avoid this from happening. Let us decode some of the most common types of online financial frauds.

Comparative Discussion Between Domestic and International Legislations Regulating Cybersecurity

Cyber security laws include rules and frameworks designed to safeguard digital systems, networks, data, and information from online threats. Countries like the US, UK, and those in the EU adopted these laws early and are continuously improving them. Meanwhile, in Bangladesh, previously Information Communication Technology (ICT) Act 2006, the Digital Security Act (DSA), 2018, and in present time the Cyber Security Act (CSA), 2023, became the primary legislation concerning cybercrime. Comparing this law with those in other countries can help us determine how well the proposed CSA aligns with international standards.

As cyber threats have evolved, numerous laws and rules emerged focusing on three key aspects

1. Protecting private, sensitive, and financial data;
2. Preventing computer-based fraud and unauthorized access; and
3. Creating guidelines to ensure strong security measures for data, computer systems, and networks across different institutions and infrastructures.

In the US, several laws are in place to safeguard specific types of data. For health data, there's the Health Insurance Portability and Accountability Act (HIPAA). For children's data, there's the Children's Online Privacy Protection Act, while the Gramm-Leach-Bliley Act deals with financial information. In Europe and in the UK, similar purposes are served by the General Data Protection Regulation (GDPR) and the Data Protection Act, respectively. In the US, computer-related frauds are addressed by the Computer Fraud and Abuse Act, while in the UK, the Computer Misuse Act criminalizes unauthorized access, computer-related frauds, and similar cyber offences [21].

Information Communication Technology (ICT) Act,2006, is one of the great initiatives to protect offences of electronic business as well as e-banking sector. Section 61 and 82 denotes the investigation process as well as penalty of accessing in restricted system Unauthorized access into any computer system knowing that it is restricted by controller of government should be treated as unauthorized access. But it is hardly being tried to locate all the probable grounds of cybercrime which is which is frequently occur at present days and which might occur in future days as well. The UK, US and the EU have qualified court banking experts to assist judges in bank related cases. But in Bangladesh there's no expert to assist judges . Also the judges and lawyers are the expert of laws, not of internet technology.

Much like its predecessor, the Digital Security Act (DSA), 2018, the Cyber Security Act (CSA) also contains sections aimed at safeguarding computer systems, networks, and data. It establishes penalties for activities such as unauthorized access, disruptions, and the improper utilization of IT systems. It also has penalties for actions like unauthorized access, disruptions, and the misuse of IT systems [22].

However, in contrast to similar laws in other parts of the world, the CSA includes clauses that do not directly relate to cyber security. These provisions include prosecuting defamation, limiting freedom of speech, and levying charges against the promotion of religious intolerance and offences related to the Official Secrets Act (OSA), 1923. The DSA gained infamy for its tendency to suppress opposing viewpoints rather than effectively addressing cyber threats, and there is no noticeable shift in this aspect in the newly enacted legislation [23].

To meet accepted standards, a law must have unambiguous provisions. Section 25 of the DSA has faced criticism due to lacking specificity and clarity, which could result in varying interpretations and possibly the unjust criminalization of legitimate criticism and opinions. Such a vague clause raises questions about whether the DSA's objective was to safeguard against cyber-attacks or if it was to curtail freedom of speech. To prevent misconceptions, any new cyber security legislation must have comprehensive and transparent descriptions of offences, aiming to eliminate uncertainties. Regrettably, the CSA does not meet this standard [24].

In the US, the Federal Information Security Modernization Act (FISMA) guides federal agencies on securing their computer systems. In the EU, the newest version of the Network and Information Security (NIS2) Directive mandates essential service providers (such as from energy, transportation, banking, and healthcare sectors) to employ proper security measures. Despite Bangladesh's DSA incorporating regulations for protecting critical information infrastructure (under Section 16), recent incidents like the NID data breach and, in the past, cyber theft from Bangladesh Bank's account, reveal the ineffectiveness of DSA and its predecessor. The new CSA could have effectively addressed this concern by incorporating stricter provisions akin to those in FISMA. Regrettably, no such additions have been made, leaving room for unsavory events to recur in the future [25].

Section 43 of the DSA, for instance, lets police arrest people without a warrant. In the US, the Computer Fraud and Abuse Act (CFAA) also allows warrantless arrests in specific cases. But it's important to note that the Fourth Amendment to the US Constitution imposes strict conditions on such actions by law enforcement. In Bangladesh, the absence of similar safeguards has led to the widespread misuse of Section 43 of the DSA, creating an environment of panic. It was prudent to either altogether remove the provision that allows warrantless arrests and searches by junior police officers or, if kept, to add more checks and balances (such as involving an executive magistrate during search and seizure operations). But the CSA has not been changed to that effect [26].

The UN Office of the High Commissioner for Human Rights has suggested removing two Sections from the DSA and changing eight others. Many of these sections primarily relate to freedom of expression and journalism, deviating from the principles outlined in the International Covenant on Civil and Political Rights [27]. But Sections 21 and 28 remain largely untouched in the proposed law. The OSA, which mostly deals with unauthorized entry to prohibited places, stealing information from there and spying (that is, offences not directly related to cybercrime) has been retained in the proposed CSA. Adding these offences to the CSA makes it more draconian than the original OSA, wherein a junior police officer could not carry out an arrest without a warrant [28].

The extent of the DSA's abuse can be gauged from the fact that, in the last five years, there have been at least 7,000 cases filed under this law, but only a few saw the accused being convicted. In the CSA, it was necessary to eliminate the provision of allowing multiple cases to be filed against

an individual for a single offence across various jurisdictions, and to also introduce rules that would severely penalize anyone, including law enforcement members, for intentionally making false allegations against innocent people. Regrettably, we see no such amendments in the CSA [29].

Loopholes in the present legal frameworks

In Bangladeshi circumstance lack and limitation of regulation of law is one of the acute obstacles to e-banking. On the other hand, in an underdeveloped country like ours, frauds were gaining significant potential which indicates a negative output in our local e-banking sector. Besides these barriers, our courts doesn't consider electronic documents as evidence, so people with a high risk of transaction were not much interested to get e-banking facilities. Technical issues were also highly connected to e-banking, but in our country technical securities were very weak an in a high risk of hacking in each moment. So, customer's trust in e-banking is still beyond imagination in Bangladesh.

1. **Lack of modern provisions in law to find out cyber crime:** As Banks in Bangladesh is governed by Bank Companies Act, 1991; but there are no provisions relating to e-banking system, cyber security of e-banking sector and how to deal with such situation. The Digital Security Act, 2018 covers the area relating to cyber security in all sectors as there are specific law by which banks are governed; it must contain expressed provisions relating to cyber security of e-banking sector because only Digital Security Act can't cover all of such sectors. Though it's an update version of law for cyber protection it has many deficiency in itself.

- Here is 30 percent laws are new but lest 70 percent are repetition of other laws like ICT Act, Penal Code and Code of Criminal Procedure.
- Where to recruit the officer to maintain the sector is not clearly define in this Act. Here also some lacking that the Police also act as also this sector and investigate it but here the IT sector specialist should recruit as a law enforcement agency to control this sector.

Again The Bankers Book Evidence Act, is another law by which our banks are regulated. This 129 year old law has been recently amended for preserving the information of a person in digital and how to inspect or present them before the courts. Provisions regarding exchanging banking information, identifying crimes and punishment and trial system. But cyber crimes should be identified separately as we are heading towards a digital nation and internet based era ; crimes are also been transformed to internet based crimes. So, not impliedly; we need explicit mentioning of cyber crimes which is still unavailable.

2. **Non appointment of experts:** The National Security Council [30] has only one person from banking sector. It is not necessary that he must be expert in internet. It is not obvious that he can identify problems relating to cyber system of a banking sector. So, such committee must include a person " ICT officer" of Central bank so that he can easily identify such emerging cyber security threats to e-banking sector.

The ICT Law 2006, though appears to be self-sufficient, it takes mixed stand when it comes to many practical situations. It loses its certainty many places like:

3. **Insufficient debate in the Parliament:** The hurry in which the legislation was passed, without sufficient public debate, did not really served the desired purpose. Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

The law even stays silent over the regulation of electronic payments gate way and segregates the negotiable instruments from the applicability of the IT Act, which may have major effect on the growth of e-commerce in Bangladesh. It leads to make the banking and financial sectors irresolute in their stands.

The Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time.

4. **Lack of knowledge of investigation officer and internet experts:** A police officer not below the rank of an Inspector of Police shall investigate any offence under this Act. This section should be modified that Inspector of police and above must have appropriate knowledge (i.e. Diploma/ Bachelor's degree in ICT related subject/ proper training in this area) [31].

Conclusion

E-Banking is a new concept in banking sector of Bangladesh. It is becoming popular in Bangladesh; thus almost all Bangladeshi banks offer many facilities of e-banking. E-banking is growing in Bangladesh day by day. Customers can withdraw and deposit money any time within 24 hours of a day. E-banking is one the major services that has made life simple and easy; a user can now do a lot of things while he is sitting on a sofa. This goes from transferring money to applying for a credit. Studies show that e-banking has multidimensional advantages for both individuals and companies, but it is not without some challenges and issues related to the security and the interest of customers [32]. Since security is considered to be one of the main preoccupations for both large and small organizations, electronic banking systems are also confronted to cyber-attacks just like any other system connected to the Internet. All types of e-banking services are being appreciated and applied by people of different walks as this eases the activities. So, if an attractive offer package provided by the government e-banking will be popular everywhere very soon. If necessary initiative can be taken like improvement of quality of e-banking service, reducing financial insecurities, reducing unemployment problem by creating IT base job for technical experts, reducing tax on e-banking equipment, close monitoring, legal provisions for controlling frauds and malpractices etc. e-banking practices will increase and more positive impact will go on the banking sector in Bangladesh. As a result, economy of Bangladesh will be benefited immensely.

The only effective way to reduce cybercrimes or data breaches is to raise awareness, people's understanding of their roles and responsibilities and to continue tightening up

the enforcement of the law. There is a key need to build a foolproof cybersecurity structure that doesn't compromise with the safety of customer's data and inancial institution's critical transactions.

A well-functioning e-banking network is dependent on availability of a backbone network connecting the whole country. Developing and implementing online banking system in a country like Bangladesh is much challenging. To improve or overcome the problems of e-banking services in the country; in addition to strengthening legal framework, there are some recommendations such as: In National security Council ; ICT officer of central bank should be included & they should meet on regular basis and Bank Companies Act, 1991 should be amended and contain provisions regarding E-banking system and emerging cyber threats of such. E-banking systems should be simple to use, fast and user friendly and Bankers Book Evidence Act should contain provisions relating to cyber crimes, punishment & trial system. Appropriate legal framework and adequate training and technological support to develop the manpower should be provided [33]. The whole country should be connected under fiber optic backbone for electronic banking infrastructure as soon as possible.

Government, in collaboration with the banks, should educate and inform its citizens and customers on the work-ability and effectiveness of E-banking. Banks should have adequate research and technological background in this regard. Bank can charge normal profit to enlarge the market size on the electronic banking products. Political commitment to improve governance and institutional strength is essential for successful application of e-banking.

References

1. C Denoel. L'e-Banking Remplace-T-Il La Banque Traditionnelle Ou La Complete-T-Il. Mémoire de Master: Sciences de Gestion: Université de Liège, 2008.
2. E. Banking, "Risk Management for electronic banking and Electronic Money Activities, 1998.
3. J Midgley. "Financial inclusion, universal banking and post offices in Britain," Area,2005:37(3):277–285.
4. C Denoel, L'e-Banking Remplace-T-Il La Banque Traditionnelle Ou La Complete-T-Il. Mémoire de Master: Sciences de Gestion: Université de Liège, 2008.
5. Lawyers & Jurists, <https://www.lawyersnjurists.com/article/trend-electronic-banking-bangladesh> accessed on 22nd February 2024.
6. Bob Batchelor. "The History of E-banking" (biZfluent, 26th September 2017). https://bizfluent.com/about-5476081-use-computers-banks.html accessed on, 2024.
7. Feinman, *et al*. Security Basics: A Whitepaper, 1999. (http:/ /www.pwc.com).
8. Financial Services Security Lab Background. Security Issues and Threats, 2001.
9. Rahman MM. Innovative Technology and Bank Profitability: The BangladeshExperience. Policy Analysis Unit (PAU), Bangladesh Bank WP 0803, 2007.
10. Azam MS. Implementation of B2C E-commerce in Bangladesh: The effects ofbuying culture and E-infrastructure. Advances in Global Business Research,2007:3(1):55-81.
11. Azam MS. Adoption of Personal Computer in Bangladesh: The Effects ofPerceived Innovation Characteristics. Proceeding of the 2nd International Conference of the Asian Academy of Applied Business (AAAB). Indonesia: AAAB, 2005, 647-655.
12. Awal MA. Internet in Bangladesh: Past, Present & A Better Future. Asia PacificNetworking Group, 2004.
13. Khan AS. Telecom Industry in Bangladesh: Current Status and Emerging Issues. Telecommunications in Bangladesh: Emerging Issues, 2001.
14. Bakta NC, Sarder MMR. Online Banking: Bangladesh Perspectives, 2007.
15. JM Hood. "Demographics of ATMs", Banker's Magazine, December-December, 1979, 68-71.
16. NB Murphy. "Determinants of ATM activity: the impact of card base, location, time in place and system", Journal of Bank Research, autumn, 1983, 231-3.
17. RE Stevens, PS Carter, RT Martin, D Cogshell. "ATM nonadopters: how valuable are they?", Banker's Magazine, September-October, 1987, 51-3.
18. LE Ostlund. "Perceived innovation attributes as predictors of innovativeness", Journal of Consumer Research,1974:1(2):23-9.
19. Index Mundi. "Facts about bangladesh," Available: http://www.indexmundi.com/facts/bangladesh
20. Abi Tyas Tunggal. "What is a cyber threat" (UpGuard, 2024. https://www.upguard.com/blog/cyber-threat accessed on 22nd May 2024
21. CSA v cybersecurity laws of other countries https://www.thedailystar.net/opinion/views/news/csa-v-cybersecurity-laws-other-countries-3405421 accessed on 22nd February 2024
22. ection- 17-23,22,30 and 32 of The Cyber Security Act, 2023
23. Ibid [21]
24. Section 25 of The Digital Security Act, 2018
25. Supra Note 21 at 11
26. Ibid
27. Section 21 and 28 of The Digital Security Act, 2018
28. Supra Note 25 at 12
29. Ibid
30. Section 12 of The Digital Security Act, 2018
31. Section 80 of The Information and Communication Technology (ICT) Act (Act No. 39 of 2006)
32. Jayaram, PN Prasad. "Review of E-banking System and Exploring the Research Gap in Indian Banking Context," Int. J. Innov. Res. Dev,2013:2(2):407–417.
33. The Bank Companies Act (Act NO. 14 of 1991)