INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Dec 2023
ISSN: 2582-6433

E BANKING IN INDIA: A CRITICAL STUDY OF LEGISLATIVE MEASURES

AUTHORED BY – DR. TANVEER KAUR

Abstract

A nation's financial sector is crucial to its overall economic growth. An economy's lifeblood is banking. A robust and sound financial system is a crucial prerequisite for economic growth. The Indian banking sector is now experiencing an IT revolution. The use of the internet in financial institutions has brought about a modernization of the industry. Both banks and customers have profited from it. Technology and creativity have brought about a lot of developments in Indian e-banking. The banking industry has seen a number of innovations, including the introduction of cards, the Electronic Clearing Service, the Electronic Funds Transfer, and the concepts of online and mobile banking. The word "e-banking" refers to a broad category that includes online, phone, and mobile banking. The bank hopes to offer the fundamentals of IT-based Enabled Services through E-Banking. It was completely distinct from the conventional banking system at the same time. Making debit and credit transactions is more convenient for the public. The growing number of individuals in India who have access to the internet is one of the factors contributing to the growth of e-banking. Because electronic banking has so many benefits, many these days choose to utilize it. However, it has also brought up some problems and difficulties related to cybercrime, such as credit card fraud, phishing, and data theft. Thus, an attempt has been made in this article to provide an overview of e-banking in India as well as the many problems and difficulties that the banking sector faces.

Key Words*: E banking, information technology, traditional banking, cyber crime, credit card fraud.*

ISSN: 2582-6433

Introduction

Banking has always been crucial for the economy, but with the advent of technology, traditional brick and retail banking has been replaced by online banking, offering convenience and flexibility for customers. E-banking allows financial transactions to be conducted online, allowing customers to access their accounts anytime, anywhere. As technology becomes more reliant, cyber regulations are becoming increasingly important to control and protect online banking. Banks must ensure system safety and compliance with relevant laws before implementing cyber restrictions. To protect customers' financial information from online fraud, strong security protocols like firewalls, multi-factor authentication, and encryption are necessary. Technology has made commerce easier for banks and their clients, but it also presents opportunities for global organized criminal networks. Despite the global village, established banking institutions face significant threats from cybercrimes.

The rise of information technology has created cyberspace, allowing anyone to access data and information through the internet. However, this has led to increased online misuse of technology, resulting in local and international criminality. Cybercrime is an unlawful action committed by using computers, electronic devices, or the internet, with penalties imposed by national statutes. Governments face challenges in preventing cybercrime due to the global reach of engineering, as cyberspace crosses national and international borders and many computer systems can be accessed from anywhere. Reliable data on cybercrime is difficult to obtain, as many cases remain unreported and unidentifiable. Cybercrime is particularly prevalent in India. This paper is an attempt to critically analyze the legislative measures put forward for the E banking.

Online Banking: A Novel Approach

Banks are the engine of the financial sector, which is essential to the economy of every country. Banking was first developed in Babylon, Mesopotamia, and Egypt about 4,000 years ago. With the advent of paper money as a medium of trade, the banking industry has experienced a dramatic transition. By 16,000 A.D., checks were being used extensively. Thanks to telegraph technology, banks were "wiring" money across locations in a matter of seconds by the mid-1900s. There have been three different periods of payment history: (1) coin and note payments; (2) paper payments; and (3) computerized payments. In addition to providing an ever-expanding array of electronic payment options, new technology has profound implications for the way banks function generally.

ISSN: 2582-6433

E-banking is the process of employing information technology to carry out banking operations. It describes how bank services are sent electronically to a customer's house or place of business. The new global reality of e-commerce is significantly changing the banking industry[1]. A contract of sale consists of three parts: the offer, the acceptance, and the transfer of consideration. One part of the transaction that banking mostly handles is the payment of money. E-commerce is now thought to be the biggest commercial window in the globe. It has resulted in a paradigm shift in the dynamics of banking and business[2].iii The global information technology revolution has not been entirely ignored by the Indian banking sector. Technology is employed in banking in four main ways.[3]:

1. To manage a significantly bigger customer base
2. Significantly lower the actual cost of processing payments.
3. To release banks from the conventional limitations of place and time and introduce fresh goods and services

Electronic technology has become essential in banking transactions in India due to communication networks like INFINET, optical fiber network, and terrestrial lines. Basic telecom service providers have expanded their networking options. The expansion of online shopping has led to policy discussions focusing on developing, administering, and controlling electronic payment systems. The need for quick, efficient payment systems has increased with new tools like credit cards, telebanking, ATMs, EFT, and ECS. India's economy benefits from straight-through processing.

E-Banking Characteristics

- Clients may access their record data, such as balances, exchange histories, and declarations, using online banking.
- Through e-banking, customers can transfer money between accounts within the same bank or other banks.
- Users may pay their bills online by manually scheduling payments or by setting up automatic

[1] S. Ganesh, Electronic Commerce: Applications in Banking", in S.B. Verma, S.K. Gupta and M.K. Sharma (edited), p. 27
[2] R. P. Nainta, Banking System, Frauds and Legal Control, Deep & Deep Publications Pvt. Ltd., New Delhi, 2005, p. 154
[3] S.S. Kaptan and N.S. Choubey, Indian Banking in Electronic Era, Sarup & Sons, New Delhi, 2003, p. 91

ISSN: 2582-6433

payments using e-banking.

- To manage their accounts, e-banking users can purchase checks online, create new accounts, and update personal information.
- Because many e-banking providers offer mobile banking apps, users may do financial transactions from their smartphones or tablets.
- To stay updated on their accounts, customers using e-banking can set up alerts and warnings, such as account balance or exchange cautions.
- To protect consumers' financial and personal information, e-banking employs a variety of security measures, including fraud monitoring, two-factor authentication, and encryption.
- Customer service is often offered by e-banking services through a number of channels, including online chat, email, and phone.

Indian laws' function in defending online banking

Legal framework for E-Banking in India

The Reserve Bank of India (RBI), which was founded in 1935 and serves as the country's ultimate monetary authority and source of all banking activity, started releasing rules, circulars, and instructions piecemeal in order to keep up with the digitalization of the financial sector. The legal foundation for banking in India is comprised of the following laws:

- The Banking Regulations Act,1949
- The Reserve Bank of India Act ,1934
- The Foreign Exchange Management Act,1999

The Banking Regulations Act of 1949 states that, in general, an organization cannot conduct banking operations in India without first getting a license from the Reserve Bank of India.[4]

To conduct business in India as a bank, a corporation must apply for a license from the Reserve Bank of India under the Banking Regulations Act of 1949. The Financial Guidelines Act of 1949 makes reference to a bank's prudential requirement as well as its capabilities and exercises. The requirements of the Reserve Bank of India Act come into play when a non-bank accepts deposits from the general public.[5]

[4] Mishra A.K., Internet banking in India. Banknetindia.com, http://www.banknetindia.com/banking/ibkg.htm.
[5] ibid

ISSN: 2582-6433

The Indian government to pass the Information Technology Act, 2OOO, and also made it difficult for banks to follow the law when it came to maintaining the privacy and confidentiality of their clients' accounts. It was also encouraged to use the internet and other electronic media for business, especially financial operations. In addition to attempting to prevent cybercrime, the demonstration acknowledges electronic markings, e-archives, and e-exchanges.[6].

The Reserve Bank of India released guidelines in 2001 for know-your-customer procedures, anti-money laundering measures, and privacy control in internet banking. Customers were therefore urged to convert to online banking, but there were reservations about security and privacy of transactions.[7]

In response to the growth of online banking and e-commerce, the Indian government sought to draft a second measure dubbed the "Personal Data Protection Bill 2006" to safeguard people's privacy, however neither chamber approved the bill. In the interim, the Act's Sections 43A and 72A were introduced in 2008 to protect sensitive personal data and information ("SPDI") as well as personal data ("PI").[8]

Except in specific situations, Indian nationals are not allowed to borrow money from, lend to, or create foreign currency accounts with non-residents, including non-resident banks, according to the Foreign Exchange Management Act of 1999 (FEMA).[9]

Laws governing e-banking

The government has legalized internet banking, and the 2008 amendment to the IT Act largely satisfied the last criteria for online transactions. The basis of online banking is acknowledged by the IT Act as being electronic transactions. Electronic transactions are agreements, contracts, and transactions that are completed online. The country's enactment of the IT Act in 2000 made e-commerce and electronic transmission lawful.

[6] Journal of Internet Banking and Commerce, www.Arraydev.com/commerce/jibc
[7] Enabling E-Commerce in India, www.giic.org.
[8] Avinandan Mukherjee, A model of trust in online relationship banking, The International Journal of Bank Marketing 2003; 21, 1; ProQuest Central p. 5 (2003)
[9] Foreign Exchange and Management Act, 1999.

ISSN: 2582-6433

1860 Indian Penal Code

Since the issue of Internet banking infractions is essentially money, various charges listed in Section XVII of the aforementioned Act's Penal Code may also be enforced in cases where the infringer commits particular offenses listed in that section pertaining to Internet banking. For this reason, the following sections are relevant in this case:

- Theft. [Ss. 378 & 379]
- Extortion. [Ss. 383 & 384]
- Criminal misappropriation of property. [S. 403]
- Criminal breach of trust. [S. 405 & 406]
- The term "forgery" has been defined in relevance to the electronic record as well, i.e. the offence of forgery is said to be committed when anyone makes not only a false document but also a false electronic record [S. 463]. The term "making of false document" also includes affixing electronic signature[10] on any electronic record. (S. 464(c)]
- Use of forged documents or electronic record and use of such forged document as genuine. [S. 47o, 471] The IT Act, 2000 has amended the original sections to add "electronic documents" in the definition of forged documents.

Cheating is when someone is tricked or dishonestly persuaded to provide property, etc. [Sections 415 and 420]. This is relevant in addition to the important provisions of the IT Act as it should be achievable via the use of technological means.

Prevention of Money Laundering Act, 2002

India has passed the Prevention of Money Laundering Act, 2002 (15 of 2003)[11] and the RBI, SEBI and IRDA art brought under the Act and thus all the financial institutions, banks, mutual funds, insurance companies and their financial intermediaries are also covered by it. The Act has since been amended in 2005, 2009 and 2012.

[10] Electric Signature, Art.2, Definition; Part I, UNICITRAL Model Law on Electric Signatures with Guide Enactment 2001, I

[11]The Act is passed as a consequence of the Political Declaration adopted by the Special Session of the UN General Assembly 1999 which called upon the Member States to adopt an anti-money laundering law and connected programmes. Accordingly, the Standing Committee on Finance presented its recommendations to the Lok Sabha on 4-3-1999

ISSN: 2582-6433

The crime of "money laundering" is committed by anybody who, whether directly or indirectly, is a party to or participates in any action pertaining to the proceeds of crime, including its concealment, possession, acquisition, use, and presentation as untarnished property. [Section 3 as modified in 2012][12]. If proven guilty, money laundering carries a strict three-year maximum sentence that can be increased to seven years in jail in addition to a fine. (Section 4 as revised in 2011, above). However, the sentence may be up to seven years if the proceeds of the crime are related to paragraph 2 of Part A of the Schedule. [Section 4]. Any property earned or generated as a result of any criminal action of any scheduled offense is referred to as "proceeds of crime" [S. 2(u)]. The definition of "scheduled crime" is defined as crimes that are included in the Schedule to the Act's Parts A and B. Part C has been added to the original Act by the Prevention of Money Laundering Amendment Act, 2009 which includes the phrase offences having "cross-border implications."

Internet banking and the Payment and Settlement Systems Act, 2007

When it comes to infractions that are subject to penalties under this Act, the Reserve Bank of India is the principal authority. Under it, offenses include running a payment system without permission, not adhering to the conditions of authorization, not producing statements, not returning information or documents, giving false information that discloses information that is forbidden, and not following RBI instructions. The following is a summary of these offenses:

Disrespect for electronic money transfer for lack of funds, etc., in the account: When an electronic funds transfer initiated by an individual from a record maintained by him is unable to be carried out because the amount of money left to the credit of that record is insufficient to honor the exchange instructions or because it exceeds the amount scheduled to be paid from that record by a contract made with a bank, it is considered an offense. The penalty that is being proposed is two years in prison, a fine equal to double the amount of money that was moved electronically, or both. Section 25.

Violation of Section 4[13]. If a person violates Section 4 or the terms and conditions of authorization

[12] The Prevention of Money Laundering (Amendment) Act, 2012, dt. 3-1-2013.
[13] Payment system not to operate without authorisation. RBI is the only authority to author- ise payment system and its operation. Any one desirous of commencing or operating a payment system should apply to the RBI. [Ss. 4 and

ISSN: 2582-6433

under Section 7,[14] he commits an offence punishable by a minimum of one month in prison and up to ten years in prison, a fine of one crore rupees or more, if any. In addition, there would be a punishment of one lakh every day for the duration that the violation persists. [Section 26(1)]. If the applicant for authorization to operate the payment system willfully makes a false statement or fails to make a significant declaration, they would be subject to a three-year prison sentence and a punishment that starts at Rs. 10 lakhs and can go up to Rs. 50 lakhs. [Section 26(2)]. If anybody fails to present any statement, information, returns, or other papers, or fails to furnish documents as required under Section 12[15] or Section 13[16] while an inspection is made under Section 14[17], then such failure shall be punished with fine up to Rs 10 lakhs in respect of each offence and if persistence continues then the fine may extend to Rs. 25, 000 for every day until such refusal, etc. continues. [S. 26(3)]. Information disclosure when it is forbidden under Section 22[18] shall be penalized by up to six months in prison, a fine of up to five lakhs rupees, or both. The maximum penalty would be two times the amount of damages resulting from the act of disclosing the information. [Section 26(4)]

In the event that a denial is made, or in the unlikely event that a default is made in response to a request or guideline made under the Act of 2007, the defaulter will be hit with a fine that could total up to Rs. 10 lakhs. If the default or negation continues, they will also be hit with an additional fine of up to Rs. 25, 000 for each day that the contradiction or default persists. [S. 26(6)]

Information Technology (Amendment) Act, 2008

A variety of other offenses have been classified as cybercrimes under the IT Act of 2000 (as amended in 2008). The following sections are briefly discussed in relation to online banking:

A business entity that handles personal data is obligated to compensate the individual for damages

5]
[14]The RBI after receiving the application for commencing or operating the payment system shall hold an inquiry [S. 6] before considering the application for operating the system. While disposing of the application the RBI can issue or refuse authorisation. If it issues it must consider: the need for authorisation, the technical standards of the proposed payment system, the terms and conditions of operation of the proposed payment system including security procedure, the manner of transfer of funds, the procedure for netting, the financial status of the applicant, the interest of consumers, monetary and credit policies, etc. [S. 7]
[15] The RBI can call for returns, documents or other information from any system provider [S. 12]
[16] The RBI shall have power to access the payment system whenever required. [S. 13]
[17] RBI has power to authorise any officer to enter any premises, make an inspection of the payment system, computer system or any other equipment to check if compliance with the orders and directions is observed. [S. 14]
[18] Duty to keep the payment system confidential. A system provider is under obligation not to disclose any document or information relating to the payment system as directed by the RBI. [S. 22]

ISSN: 2582-6433

if it fails to protect them. Rule 8 of the IT Rules, 2011 now specifies security policies and procedures that must be followed while managing such personal data (Section 43A). It was absent from the Amendment Act of 1988. International Standard IS/ISO/IEC 27001 on "Information Technology-Security Techniques-Information Security Management System Requirements" is one example of such a standard.

Identity theft: Using another person's electronic signature, password, or unique identification number unlawfully or dishonestly is punished by up to three years in jail and a fine of one lakh. (Section 66C)

It is illegal for intermediaries to fail to preserve and keep information in accordance with the authorized procedures. Penalties include fines and up to three years in jail (Section 67C).

Information disclosed by a body with access to it without the subject's permission. The penalty might be two years in prison, a fine of up to one lakh rupees, or both. In accordance with Regulation 2O11, a body corporate is required to get the permission of the individual in question with respect to the type and purpose of the information being collected (Section 70).

A body corporate that requests personal information from an individual under contract and discovers that it is being used to intentionally harm or deceive another party can face up to three years in prison, a fine of up to Rs. five lakh, or both (Section 72A).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[19]

The Rules mainly deal with the personal information of users and are a counterpart to the IT Act of 2000. Therefore, in the context of Internet banking, the password and electronic instructions sent to the bank by the account holder comprise the user's personal information. Consequently, the following words are defined in the Rules:

A passphrase, code, secret word, encryption key, or decryption key is a type of word or phrase that is used as a password to get access to data. [R. 2(b)].. Any information on a natural person

[19] G.S.R. (E) The Gazette of India, Extra., Part II, S. 3, sub-s. (i), dt. 11-4-2011. The Government of India, Ministry of Communications and Information Technology, New Delhi

ISSN: 2582-6433

(human being) that is available with a body corporate and adequate to identify such a person is referred to as "personal information". [R. 26]

"Sensitive personal data or information" refers to personal data that is associated with a password, financial data that includes details of a bank account, credit card, debit card, or other payment instrument, biometric data, or other personal data that a body corporate has lawfully received. [R. 3]

Only with the permission of the information source and even then, for a legitimate reason, may the body corporate collect personal information, including sensitive personal data. [R. 5]

Risks Associated with Online Banking

Computer crime has existed for as long as computers. Any new development or discovery has the potential to be put to both beneficial and detrimental uses. While the majority of people use PCs for ethically sound and constructive purposes, some people use them for heinous, exploitative, or illegal purposes. A computer-related crime is referred to as "Computer Crime." Three broad classifications are used to categorize PC infractions.:[20]

- Crimes Associated with Data; Crimes Associated with Software; and Physical Crimes.

The ecosystem of the Internet makes it very easy to direct illicit actions on computers. These are referred to as cybercrimes, or crimes committed via the Internet. The term "cybercrime" has recently gained popularity as a catchy way to describe a variety of online safety concerns. Cybercrime refers to actions of any type carried out with a criminal intent in cyberspace or via the internet. These may be workouts that have lately evolved with the growth of the new media, or they could be crimes in the old faculties. Any movement that basically transgresses human rights may be associated with the scope of cybercrimes..[21] Inventive prisoners use a variety of methods and "stunts" to defraud innocent people of their money, buy things without paying for them, sell things without a delivery, abuse people, and much more. With its global reach, the Internet has also contributed to an increasing amount of cross-line deception. When introducing online business exchange through E-Banking, there are a lot of concerns that need to be

[20] R.P.Nainta, pp. 59-60
[21] Definition by Advocate Pavan Duggal

ISSN: 2582-6433

addressed.

Financial crimes using the Internet are becoming more and more prevalent in the e-banking sector. One of the key concerns that must be addressed before using e-banking is security. Significant risks include unauthorized access, data loss or damage from hackers, data loss and damage from viruses, and unauthorized access within the company.[22] An company using the Internet to conduct online payments runs the risk of losing security. For the protection of consumer rights, confidentiality, integrity, authenticity, reliability, and privacy are crucial considerations.[23]

Phishing is an online scam where unsuspecting individuals are coerced into divulging personal information such as usernames and passwords, which spammers then use for unauthorized purposes. The basic tactic of phishing is to send emails purporting to be from buyers' banks or other financial institutions that are in default, claiming to have the buyer's personal information at this point. The customer is then contacted to confirm the details by clicking on a single link (URL) provided in the fraudulent email. This URL directs the buyer to a phony website that looks and feels much like the legitimate website. The data the customer provides in the forms on the phony website is collected and used to perpetrate extortion in their records, charge cards, or other accounts.[24]

Pharming is a type of online fraud whereby a considerable number of unsuspecting individuals are tricked into visiting malicious websites instead of the intended web-based financial services. The fictitious locations, to which victims are taken without their knowledge or consent, are expected to have an appearance similar to that of an actual one. However, when users input their secret phrase and login name, thieves obtain the data.[25]

The word "hacker" is commonly used to describe an outsider who gains access to a computer system. Two categories exist for hackers. White- Hat Hackers engage in moral hacking, testing their clients' frameworks to identify weak points that may be addressed. Dark-Hat Hackers, sometimes referred to as crackers, are thugs. A malicious hacker known as a "Cracker" may target

[22] V.P. Shetty, “Electronic Banking”, in S.B. Verma, S.K. Gupta and M.K. Sharma (edited), p. 24.
[23] S.Ganesh, p. 31.
[24] S.C.Gupta, “Internet Banking-Changing Vistas of Delivery Chanel”, in S.B. Verma, S.K. Gupta and M.K. Sharma (edited), p. 106.
[25] S.C. Gupta, p. 106.

ISSN: 2582-6433

a challenging problem for a collaboration.[26] The updated IT Act of 2000 does not define hacking. However, a hacker may face penalties under Section 43(a) read in conjunction with Section 66 of the Information Technology (Amendment) Act, 2008, as well as under Sections 379 and 406 of the Indian Penal Code, 1860.

Identity theft, a growing problem in cybercrime, is when a criminal assumes the identity of another person. The fraudster uses charge card information and federal retirement aid numbers, which are usually obtained online, to commit fraud (e.g., to make purchases or use services) that the victim could be required to pay for.[27]. A technique called "trap door" looks at hacking software code to allow for the insertion of extra instructions.[28]

Cookies are small text files that are downloaded to a user's computer when accessing a website. They include information supplied to the user's software by the site server. A web user may occasionally view cookies in the header source code of a website page whenever they so want. The recently stored data will be sent to the website by the user's internet browser should they return to it. In this way, cookies are able to recognize the website as the same machine that was present a while ago, tracking the advancements of individual computer users. Most cookies are made up of code or other information that uniquely identifies a user's machine; this allows the website to monitor and record the user's activities both on the website and in other places. Instead of specifically identifying data in the cookies itself, websites may be able to identify the user whose application sent the goodie.[29]

Cyber security for E-Banking in Banks

Methods and instruments to monitor, fix, and improve the security of applications using firewalls, encryption, and antivirus programs after they are deployed. Solutions to safeguard the company's IT stages, network connections, server farms, and linked gadgets, among other things. Devices that guard sensitive, private, and confidential data from abuse, illegal access, disclosure, damage, alteration, and disruption. Technologies and security protocols are among the devices used to protect distributed registration environments from internal and external cyber attacks. Network

[26] Efraim Turban, et.al, Electronic Commerce, Prentice Hall, Upper Saddle River, NJ, 2006, p. 118
[27] Efraim Turban, 2006, p. 648
[28] See: P. Weill and M.R. Vitale, Place to Space: Migrating to e-Business Models, Harvard Business School Press, Boston, 2001.
[29] Lee Fen Yem, Cyber Space Law, Oxford University Press, New Delhi, 2007, p. 128

ISSN: 2582-6433

users' responsibilities and access rights are defined and managed by an architecture or security rules that are implemented to safeguard sensitive and important data. Embracing the RBI's recommendations for the cyber security architecture, which center on three points: Cyber security and resilience, the Cybersecurity Operations Center (C-SoC), and Cyber security Incident Reporting (CSIR) entail informing staff members and outside services about the significance of safeguarding private data and taking precautionary steps to prevent cybe rattacks..

Hacking in the Banking Industry

One of the third-biggest private sector banks in India, Axis Bank, had a data breach in 2016 that resulted in the exposure of its clients' personal data, including credit card and bank account information.[30]. The biggest public sector bank in India, State Bank of India (SBI), was the subject of a phishing scam in 2022, in which fraudsters impersonated the bank and sent phony SMS messages requesting that users update their PAN and KYC information. Several clients lost money as a result of falling for the hoax.[31] Cybercriminals used phishing scams in 2020 to target ICICI Bank clients, posing as emails and texts and requesting personal and banking information. Several clients lost money as a result of falling for the hoax. One of the biggest banks in India, HDFC Bank, had a cyber attack in December 2019 that had an impact on its online banking services. In an effort to stop more harm, the bank was forced to temporarily halt its online banking services. Cybercriminals used a phishing scheme in 2021 to target Kotak Mahindra Bank clients, posing as emails and texts and requesting personal and banking information. Several clients lost money as a result of falling for the hoax.

Conclusion

Banking has become a reliable and strong base for handling finances and financial issues, with India's banking sector experiencing social and financial transformation since independence. The rise of the internet and computers has transformed the banking industry, allowing for greater interaction with various cultures and sub-societies. However, the internet can also be a virtual damnation when misused or abused by those with bad intentions. E-banking has revolutionized

[30] Bank Informs Rbi of Security Breach: Axis Suffers Cyber Attack, Hires Ey To Probe Damage - The Economic Times, https://economictimes.indiatimes.com/industry/banking/finance/banking/axis-bank-yet-to-figure-outextent-of-server-breach-damage-if-any/articleshow/54927032.cms

[31]SBI alerts about online KYC fraud: Tells customers how to keep bank account safe - The Economic Times https://economictimes.indiatimes.com/wealth/save/sbi-alerts-about-online-kyc-fraud-tells-customershow-to-keep-bank-account-safe/articleshow/84370088.cms?from=mdr

ISSN: 2582-6433

the banking industry, providing convenience and freedom for customers. However, this also requires the protection of consumers' financial information. Cyber regulations are essential to ensure the security of online banking systems and consumer privacy. India lacks an explicit E-Banking Regulation, despite RBI instructions and the Information Technology Act, 2000 providing some indirect provisions. Indian banks struggle with cyber security and must separate to maintain a technologically and legally sound e-banking infrastructure. Resistance to internet banking slows adoption and forces banks to maintain their current customer service options, reducing their ability to fully utilize technological innovations. Bank supervisors must recognize these issues to design strategy steps to remove barriers and ensure e-banking remains popular, providing flexibility and convenience to institutions and clients.

Recommendations

Banks' Data Privacy and E-Banking:

- Adherence to data privacy laws like GDPR is crucial for secure data collection, storage, and processing.
- Regular security mechanisms and regulatory environment are necessary for Internet Banking.
- Banks should keep users informed about complex technologies and changes.
- SMS alerts and Secure Socket Layer (SSL) to ensure information confidentiality.
- Prioritizing cyber security evaluation, controlling remote access, restricting third-party access, adopting technological solutions, raising awareness, and improving threat detection and response capabilities are essential.