CYBERCRIME IN INDIA IN THE CONTEXT OF THE BANKING INDUSTRY: A CRITICAL ANALYSIS OF CUSTOMER PERCEPTION.

[1]KUKU RAM KANOJIA, [2]DR.RAJESH KUMAR SINGH
[1]Ph.D. Student, Parul Institute of Law, Parul University, Vadodara
Advocate and Former General Manager, Bank of Baroda
Email ID kr.kanojia@gmail.com
[2]Associate Professor, Parul Institute of Law, Parul University Vadodara

Abstract
Globalization has made online banking an essential part of 21st-century life. His social relevance drove him to devise several means to communicate information, ideas, and expertise. New e-banking technology makes transactions quick and rapid with a click. Daily banking is easy with digital banking. Misuse of information technology in cyberspace is spawning national and worldwide cybercrime. Risks and challenges rise. The two principal regulations governing real-time electronic surveillance in other criminal investigations permit the use of search warrants to obtain access to the suspected crime scene of the burglar. As examples of evidence, the software utilized to illicitly access the system and the computer employed in the commission of the offense are also present. Present study examines cyberspace and customer perceptions of cybercrime. The survey found that customers need to be aware of cybercrime in online banking and personal financial data and how to protect themselves.
***Keywords**: Consumer perception, Internet banking, cyber-attacks, hacking, mobile banking, online banking.*

INTRODUCTION

The financial sector is essential to every economy. A flourishing banking sector is crucial to the current and future of any economy. In this technological era, the goal cannot be accomplished using conventional banking methods. In order to withdraw cash, deposit a check, or seek a statement of accounts, every individual must physically visit the branch. Offering online banking is moving from "nice to have" to "need to have" status. Therefore, net banking has become the standard rather than the exception in many industrialized nations as a result of its low cost.

Cybersecurity has been in the news a lot recently, appearing in publications, on company websites, and in social media. Consequently, the Internet is seen as untamed cyberspace, a platform for various activities such as commerce, consumption, business, and pleasure. Still, the occurrence has grown in frequency in industries dealing with digital transactions, like the financial and telecommunications industries. In spite of the ever-present benefits of Information and Communication Technology (ICT), the idea of cybersecurity threat is a major factor in whether or not people would use and keep the technology (Tyagi, 2019). Customers' attitudes regarding adopting and maintaining relationships with new technologies may be moderated, in part, by the increasing understanding of the concept of cyber threat. There is a direct correlation between the user's choice of technology and the underlying notion (cyber-threat) in the research issue, which signifies the negative effects of using ICT. According to previous research (Kimani et al., 2019), the banking industry is particularly susceptible to cyberattacks because of the sensitive information that customers and the bank itself store online. This research has practical significance as it examines the tremendous growth in cybercrimes from the perspective of customers. The research's results and recommendations will aid financial institutions in developing and implementing policies to reduce the prevalence of cybercrime, raise public understanding of the benefits of online banking, and inspire more customers to use these services so that everyone can be benefitted. New information and empirical evidence will be added to the current literature by the results of this investigation.

CONCEPTS OF DIGITAL BANKING

New commercial and social facets have emerged as a result of forward-thinking digital technology and ways of thinking. In addition to providing high bandwidth to every area of the nation, the Indian government is actively encouraging technology adoption and upgrades as part of the country's digital transformation. Bankers can get the solutions they need for both their immediate and future technological and commercial needs through digital banking.

Nowadays, businesses are aiming to improve customer happiness and value by utilizing digital banking and information technology. This may be achieved through unified customer experiences, speedier output, operational efficiency, and more. Customers may take advantage of banking services whenever and wherever they like thanks to digital banking transformation, which also improves the customer experience. In terms of architecture, the advent of digital banking has been revolutionary. A digital banking system's viability hinges on its operational design, technological advancement, user-friendliness, informative functional design, and, most crucially, security.

Concept of Cyber Space and Cyber Security

Cyberspace refers to the intangible realm where information is exchanged and communication occurs among computer systems and networks. Every internet-connected gadget has immediate access to cyberspace, enabling various daily activities including sending and receiving emails and messages, as well as paying bills. Cybersecurity refers to the measures used to protect information and assets that exist in cyberspace. This is particularly crucial in the commercial realm, where valuable information assets are stored on increasingly intricate computer systems, necessitating even more advanced defense mechanisms.

LITERATURE REVIEW

Anwesha Ghosh's (2018) study asserted that internet banking was favored due to its convenience, cost-effectiveness, and efficiency. Financial organizations incentivized users to utilize online banking by providing discounts and additional amenities. Online banking offered financial companies the advantage of reducing costs associated with office setup and staff. Furthermore, manual transactions required more time to process, which was why both financial institutions and clients favored cashless transactions due to their relatively cheaper operational expenses. The risks associated with internet financial transactions were found to exceed the advantages. Individuals experienced anxiety at the potential loss of their financial resources. This report elucidated the diverse advantages of internet banking and the reasons behind its increasing popularity among Indians. It demonstrated the prevalence of risks associated with internet banking, which surpassed the advantages and instilled fear of financial loss among individuals. It implied that crooks exploited the lack of awareness or insufficient understanding about the dangers. Hence, it was imperative to educate and raise awareness among individuals regarding cybercrime. Nevertheless, the authors failed to propose any particular remedy for generating awareness among individuals.

In her study, S. Kalpana (2018) highlighted the fact that the affordability of broadband services and smartphones has enabled universal internet access. It became possible to gain entry to cyberspace and establish virtual connections with millions of online users worldwide. Simultaneously, it rendered individuals susceptible to cybercrime hazards. An insignificant oversight in managing digital lives could provide opportunities for cybercrimes and consequently result in financial detriment. It was imperative that caution and attentiveness were exercised when engaging in digital interactions with the external world, be it for financial transactions, social networking, gaming, online searches, and so on. This presentation offered a comprehensive examination of cybercrimes and the process of becoming a victim. Currently, it was inconceivable for anyone to abstain from utilizing internet banking; nonetheless, it was important to acknowledge the substantial level of risk associated with it. The paper proposed that lawmakers should exercise vigilance and impose stringent penalties on criminals in order to mitigate cybercrime. The government should rigorously enforce the laws pertaining to this matter. Additionally, it proposed the dissemination of knowledge and consciousness.

In his work, statistical data was provided by V.K. Bakshi (2019) to illustrate the benefits of the growing adoption of e-banking. The text outlined the function of the Reserve Bank of India (RBI) in enhancing the effectiveness of electronic banking. Additionally, the limitations of electronic banking were exposed, primarily its susceptibility to cybercrime. The necessary measures that banks and their clients should adopt were proposed, with emphasis placed on the importance of raising knowledge among customers regarding their responsibilities and rights. Additionally, the significance of international collaboration was highlighted.

In his paper, Delroy A. Chever (2019) suggested a research model that could assess the impact of cybercrime on discouraging the adoption of e-banking in the financial industry. The aim was to encourage other academics to perform empirical research in this specific area. The author presented a paradigm that would facilitate subsequent researchers in discovering potential solutions. The emphasis was placed on the three primary categories of cybercrime or frequently employed methods of operation. Furthermore, it signified a detrimental effect of cybercrime on the utilization of electronic banking. Nevertheless, the text failed to present any resolution for the issue of cybercrime.

In his paper, Kumar. D (2019) discussed the prevalent occurrence of elderly individuals falling prey to cyber theft. Elderly individuals were being targeted through phone calls when they were asked for their One-Time Password (OTP). Banks notified individuals of the need not to disclose the One-Time Password (OTP).

In a study conducted by S.Kulshrestha(2019), it was stated that cybersecurity has become increasingly crucial. Despite efforts to keep up with emerging technologies such as artificial intelligence, there is also a significant need for innovation and development of applications to enhance cybersecurity in the commercial sector. Technological advancements have facilitated the integration of cybersecurity measures into several elements, yet hackers are also leveraging these same technologies, including artificial intelligence, to carry out cybercrimes. Criminals and hackers are developing corresponding countermeasures using similar technologies. The progress has not only enhanced cybersecurity, but it has also been deeply integrated with cybersecurity at several levels, to the extent that it is now a small part of the national security discussion. The paper discusses the positive impact of technological advancements on cybersecurity, while acknowledging that these same advancements can provide benefits to criminals. Artificial intelligence is enhancing and fortifying national security. The article does not address preventive measures regarding the utilization of artificial intelligence by criminals.

In his study, Victor Lase (2020) discussed the numerous benefits that ICT has provided. ICT simplified lives by facilitating processes through sorting, coding, summarizing, and personalizing. Nevertheless, it outlined the unexpected repercussion it resulted in, specifically in the form of cybercrime. Cybercrime infiltrated various businesses, with banking being the most severely affected. Commonly employed techniques for perpetrating cybercrimes included ATM fraud, phishing, identity theft, and denial-of-service attacks (DOS). The article explored the issue of cybercrime inside the banking industry and its repercussions on financial institutions. It aimed to evaluate the cybercrime landscape and identify the individuals or groups participating in the situation. The article also analyzed the various forms of cybercrime targeting the financial sector and investigated the underlying motives behind them.

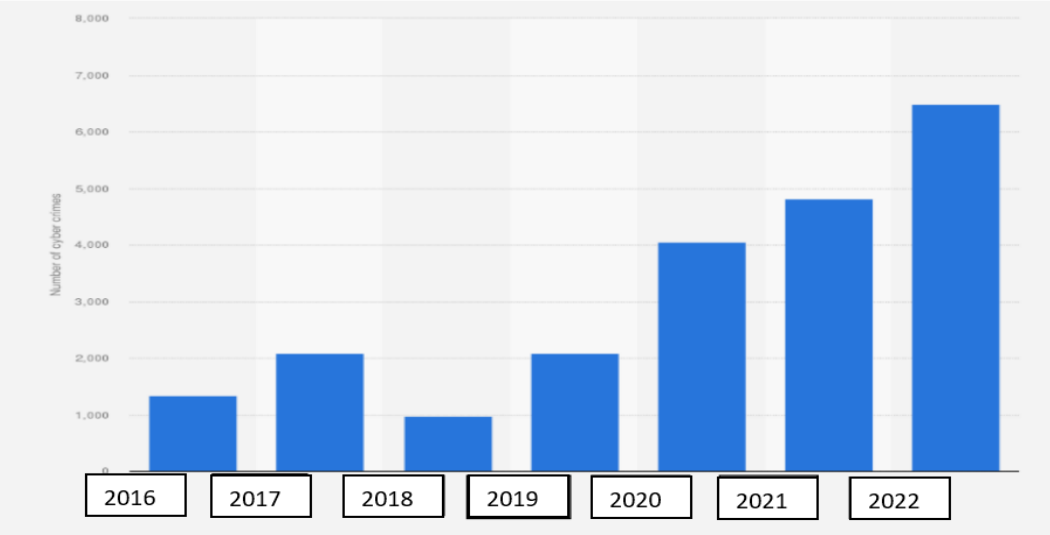

Figure 1: online banking cybercrimes across India. Source: Statista2024[1].

CUSTOMER PERCEPTION

According to a survey conducted by Mishra (2022) with 220 respondents, it was determined that comprehending and recognizing security concerns is crucial when using online banking services. The confidence level of internet banking users is assessed. When engaging in online banking and other services, it is crucial for customers to be cognizant of the prevailing dangers posed by computer fraudsters and criminals. Cyber criminals employ various tactics and strategies, including computer hacking, phishing, vishing, identity theft, denial of service attacks, social engineering, and more, to illicitly get the financial information of individuals. Hence, it is crucial for online banking clients to possess knowledge regarding the approaches and procedures employed by computer fraudsters. However, only 23% of the survey respondents verified their awareness of all the hazards highlighted in the research survey. This data demonstrates that nearly 77% of online consumers have minimal or no knowledge of the potential risks that exist for both individuals and the banking industry. This creates additional opportunities for computer criminals and fraudsters to get unauthorized access to customers' information and exploit it for unlawful activities and purposes. Online banking consumers must exercise more caution while engaging with financial services. Nevertheless, a significant majority of users, specifically over 63%, lack the ability to recognize and effectively manage the current information security risks. Moreover, over 65% of customers do not exercise any additional caution when engaging with online financial services.

According to the research conducted by S. Sudha et al (2024), cybercrimes have emerged as a significant concern in the modern world due to the widespread adoption of online and digital platforms. A significant proportion of respondents in Chennai are utilizing online banking for their financial operations. Cybercrimes primarily impact a minority population. However, the majority have implemented precautionary measures to protect themselves from cybercrimes. The majority of respondents refrain from sharing their OTP or PIN numbers with anyone and believe it is advisable to utilize PIN numbers. Individuals must employ digitalized techniques as it is the prevailing pattern in every aspect of existence. Despite the presence of safety measures, such as strong encryption, there remains a significant number of hackers, phishers, and unauthorized individuals who are illicitly obtaining our sensitive data and engaging in fraudulent behavior. It is vital to comprehend and safeguard ourselves against cybercrimes. Individuals should possess knowledge about all forms of cybercrimes. The Government should implement initiatives to educate the public about e-crimes and the corresponding safety precautions.

Case studies

The 2017 cyberattack on the Union Bank of India (UBI) was a sophisticated phishing attempt in which the perpetrators pretended to be from the Reserve Bank of India (RBI) in order to gain access to the bank's systems. Only a small percentage of people who work in customer service, online banking, or related fields actually got the malicious software-laden email. According to Tiwari (2019), just a small number of people observed the strangeness and reported it to the security team. They reasoned that the file extension (.xer rather than pdf) could have tainted its authenticity, despite the email having been forwarded from RBI. Notably, the email was opened by a small number of less tech-savvy individuals; shortly thereafter, malicious software infiltrated the networks and systems of the banks, enabling cybercriminals to attempt to take approximately $200 million. Despite the failure of the cybercriminals' endeavor, the fact that they managed to identify vulnerabilities in the financial system remains alarming. Criminals were able to breach the bank's system despite its many defenses because they identified a vulnerability and used it as a springboard. Obtaining financial information and stealing money were the main objectives of this attack.

Malicious attack on Pune's Cosmos Bank in August 2018 is another prime example of malware assault in India. Here, the internal financial system and the ATM were both put at risk. The fraudsters utilized a variety of core code exploits to move between the primary and secondary financial systems of the bank. The algorithm essentially linked a client's transaction orders with imaginary payment transfer transactions. A total of four hundred and fifty counterfeit debit cards issued in several countries were used to make large withdrawals from ATMs after the perpetrators made fake modifications to the target customers' account balances and issued fake standing-in requests, among other things.

Criminals compromised the ATM/POS system by inserting malicious software, which rendered all client requests for transactions at these locations invalid (Datta et al., 2020). The system was successful since it confirmed the transaction by sending a message to the same client after satisfactory verification. Every time a user requested a transaction at an ATM or point-of-sale system, the malicious software would send a fake return message.

CONCLUSION

Cybersecurity issues pose ongoing challenges to the dependability and security of online banking and transactions. Various types of hazards exist in the globe, include deceptive phishing attempts, covert malware, and data breaches. Phishing attacks deceive individuals into revealing personal information by utilizing fraudulent emails or websites. Devices are susceptible to malware infections, including ransomware, which can lead to financial theft or the hijacking of machines. Data breaches compromise the confidentiality of personal information, hence increasing individuals' susceptibility to fraudulent activities and identity theft. These hazards not only result in significant financial losses for individuals and enterprises, but they also endanger the fundamental confidence that supports online banking systems. Public collaboration is crucial in combating security threats. Users, regulatory agencies, cybersecurity specialists, and financial institutions should collaborate. The three fundamental components of this collaboration involve the exchange of intelligence about potential risks, the establishment of regulatory frameworks, and the promotion of innovation. Rigorous legislation ensures strict compliance with security protocols, strengthening the online transaction ecosystem. Continuous innovation is crucial for security systems and processes to effectively adapt to the evolving tactics employed by cybercriminals. Through collaboration, we can establish a resilient ecosystem that deters cyberattacks and enhances confidence in online banking services.

RECOMMENDATIONS

- Internet banking users should employ robust passwords and utilize distinct combinations of usernames for various websites and accounts.
- Law enforcement should maintain a strict and regularly updated system to monitor such offenses.
- Fast-track mobile courts should be established to expedite the resolution of these matters, address grievances, and instill confidence in the public.

- Government should monitor network activities using Big Data Banks.
- In order to mitigate the impact of these concerns and hold the attackers accountable, it is imperative to implement punishments and fines in a systematic manner.
- It is necessary to commence Awareness Programs to educate the people about the current situation and future risks.
- The public should report information about these crimes directly to the Cyber Crime Branch instead of solely relying on banks, in order to expedite and enforce stringent penalties.

REFERENCES

1. Tyagi, S. (2019). Cybercrime overwhelming online banking: A Project Management approach's alternative1, 2.
2. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25, 36–49.
3. Bakshi, V.K., Neeta, M.S. (May 2019). Cybercrime in banking sector. Aayushi International Interdisciplinary Research Journal (AIIRJ). ISSN:2349- 638x. https://aiirjournal.com/uploads/Articles/2019/05/3799_08.Ms.Neeta%20&%20Dr.%20V. K.Bakshi.pdf
4. Anwesha Ghosh,(Jan 2018), "Cyber Frauds in Banking"https://www.scribd.com/document/368465663/Cyber-Frauds-in-Banking
5. Delroy A. Chevers, (2019), "The impact of cybercrime on e-banking: A proposed model", CONF-IRM 2019, proceedings International Conference on information resources, https://aisel.aisnet.org/confirm2019/11
6. S. Kalpana and M. Mahalakshmi. (2020). A Growing Threat to Indian E-Banking Sector."JETIR December 2020, Volume 7, Issue 12. www.jetir.org (ISSN-2349-5162
7. S. Kulshrestha, (2019) "The Interweaving of Cyber security and Artificial Intelligence", IndraStra Global Vol.05, Issue No: 06.
8. Mishra, Binayee & Journals, Crdeep. (2022). Cyber Threats in E-Banking & its Effect on Consumers' Behaviour: An Analytical Study. 10.13140/RG.2.2.33218.25282.
9. S. Sudha, A. Meera, R. Aarthi Alamelu (2024). A Study on Customers' Experience On Cybercrimes And Its Protection Measures in Chennai. Proceedings of the 3rd International Conference on Reinventing Business Practices, Start-ups and Sustainability (ICRBSS 2023), DOI: 10.2991/978-94-6463-374-0_76
10. Tiwari, R. (2019). Contribution of Cyber Banking towards Digital India: AWay Forward. *Khoj: An International Peer Reviewed Journal of Geography*, *6*(1), 46–52.

Webpages

1. Victor Lase, (Aug 2020), "Cybercrime in the Banking Sector in Digital Era" https://www.academia.edu/36766879/
2. Kumar, D., (2019). "What RBI needs to do to save senior citizens from cybercrimes" The Economic Times.

Conference Paper

1. Datta, P., Tanwar, S., Panda, S.N. and Rana, A., 2020, June. Security and Issues of M-Banking: A Technical Report. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1115-1118). IEEE.