ANALYSING CYBER FRAUDS AMONGST CUSTOMERS IN E-BANKING IN MUMBAI

Adnan Tambawala[1]

[1]H.R. College of Commerce and Economics, HSNC University, Mumbai, India.

DOI: https://www.doi.org/10.58257/IJPREMS36713

ABSTRACT

Cyber fraud is a prevalent and serious threat globally, fueled by the rapid growth of the cyberworld, which has made personal and financial information increasingly vulnerable to attacks.Fraudsters exploit online data through various means, often using it for financial gain or to fund illegal activities, including terrorism.

Major incidents illustrate the scale and impact of cyber fraud, such as the 2013 Target breach affecting 40 million customers, the 2014 Home Depot breach compromising 56 million credit card numbers, and the 2015 US Office of Personnel Management hack that exposed sensitive information of over 20 million people.

Cybercriminals typically use tactics like phishing emails and malicious software to access private information. To protect against these risks, individuals and organizations should be cautious of unsolicited requests for sensitive information, verify contacts independently, andunderstand that banks will never ask for account details via email or phone.

1. INTRODUCTION

Information technology is one of the most important facilitators for the transformation of the Indian banking industry in terms of its transaction processing as well as for various other internal systems and processes.

The technological evolution of the Indian banking industry has been largely directed by the various committees set up by the RBI and the government ofIndia to review the implementation of technological change. No breakthrough in technology implementation was achieved by the industry till the early 80s, though some working groups and committees made stray references to the need for mechanization of some banking processes. This was largely due to the stiff resistance by the very strong bank employee unions. The early 1980s were instrumental in the introduction of mechanization and computerization in Indian banks.

This was the period when banks, as well as the RBI, went very slow on mechanization, carefully avoiding the use of ‘computers’ to avoid resistance from employee unions. However, this was the critical period acting as the icebreaker, which led to the slow and steady move towards large-scale technology adoption. The first blueprintsof adaptation of IT in banks were drawn with the establishment of a “Working Group “to consider sider feasibility of introducing MICR/OCR Technology for Cheque Processing under the

Chairman-ship of Dr.Y.B.Damle, Adviser of Management Services Department, Reserve Bank of India. The technological evolution of the Indian banking industry has been largely directed by the various committees set up by the RBI and the government of India to review the implementation of technological change. No breakthrough in technology implementation was achieved by the industry till the early 80s, though some working groups and committees made stray references to the need for mechanization of some banking processes. This was largely due to the stiff resistance by the very strong bank employee unions. The early 1980s were instrumental in the introduction of mechanization and computerization in Indian banks. This was the period when banks as well as the RBI, went very slow on mechanization, carefully avoiding the use of computers to avoid resistance from employee unions.

2. REVIEW OF LITERATURE

Douglas and Loader (2000, Cybercrime: Security and Surveillance in the InformationAge) Douglas and Loader in their paper stated that” Cybercrime can be defined as computer- mediated activities conducted through global electronic networks which are either illegal orconsidered illicit by

certain parties. In the banking sector, the cybercrimes that are committed using online technologies to illegally remove or transfer money to different accounts are tagged as banking frauds. Cybercrimes according to Wall (2001) can be categorized into four major categories i.e., cyber-deceptions, cyber- pornography, cyber- violence, and cybertrespass. Banking frauds are sub-categorized in cyber-deception which can be defined as immoral activity including stealing, credit card fraud, and intellectual property violations. Banks are likely to remain top cybercrime targets. Mass-market attacksagainst all industry sectors remain common, but these are believed to be relatively unsuccessful within the finance industry.

Goodman M.(2015, Future crimes: How our radical dependence on technologythreatens us all) According to author Marc Goodman, the shadowy "Crime Inc." (a catch-all term for all that is malicious on the Internet) is a virtually unstoppable force that, combined with the trend toward a global Internet of Things, leaves us more susceptible to criminal activity than ever.What's worse—we are complicit in our own exploitation, wantonly sharing our personal andprivate information online, while ignoring the maxim "If you're not paying for it, you're not the customer, you're the product." Reviewer Dov Greenbaum welcomes this well-researchedwhirlwind tour of Internet-based crime and offers some suggestions to help readers avoid falling victim to the criminal capers described in Future Crimes

3. RESEARCH OBJECTIVES

- To study cyber fraud in E-banking
- To study the various concepts related to e-banking and cybercrimes
- To study the categories of cybercrimes in e-banking
- To suggest preventive measures and safety tips to control and prevent cybercrimes
- To examine the role of different types of cyber fraud
- To evaluate the cost relationship between cybercrime and E-banking

Hypothesis

H1: Lack of security impacts consumer readiness for e-banking services.

H0: Lack of security does not impact consumer readiness for e-banking services H1: Cybercrime is considered a boon in Ebanking.

H0: Cybercrime is a disadvantage in E banking

H1: There is an awareness among people regarding cybercrimes H0: There is an unawareness among people regarding cybercrimes H1: The impact of cybercrimes is clear

H0: The impact of cybercrimes is not clear

Secondary data

The Indian banking industry has expanded its distribution channels significantly beyond traditional branches, leveraging ATMs, internet banking, mobile banking, telephone banking,and card-based systems to provide convenience and access for customers. This shift from conventional to convenience banking has been driven by IT adoption. ATMs emerged in the early 1990s, initially introduced by foreign banks and later adopted by public sector banks, allowing 24/7 access and serving as virtual branches. Innovations like biometric ATMs, multilingual ATMs, and multifunctional ATMs further enhance accessibility for a diverse customer base, including rural and less literate populations. Network switches facilitate connectivity between ATMs of different banks, offering seamless service. Internet banking, adopted since the early 2000s, has progressed to fully transactional services, enabling anywhere, anytime banking and significantly reducing transaction costs. Mobile banking allows real-time updates and multiple transactions through mobile devices.Similarly, phone banking offers 24-hour access to essential banking services. Card-based systems, including credit, debit, and smart cards, have grown in popularity, aided by ATM and POS networks. Emerging technologies like satellite banking aim to bridge connectivity gaps in rural and remote areas, while NEFT and RTGS facilitate electronic funds transfers and high-value transactions nationwide. These advancements are transforming Indian banking into a moreaccessible, efficient, and customer- centric industry.

Findings

- Now-a-days majority of people prefer online banking considering advantages such as24/7 Availability, ease of process, speed and efficiency.
- Most of the people think that e-banking is the efficient way to deliver bankingservices.
- Electronic Fund Transfer, Debit Card and ATM service are the most preferred E-banking services.
- Because of lack of trust, friction and risk of losing money, some people are not usinge-banking services.
- Many different kinds of attempts are being made for gaining personal banking information from users. Some users get trapped and become victim of cyber frauds.
- Banks have started different initiatives for spreading awareness within consumers andalways ask their consumers to stay vigilant when they are being approached for acquiring personal banking details.

Limitations

- The personal bias of the respondents might have an impact on the data collected due torespondent’s reluctance to answer the question.

- The study is restricted to Mumbai. Hence it may not be possible to generalize thefinding to the entire population of the country.
- Primary source of data collection: Primary source of data is the main source of gathering information, hence manipulation at the respondent's end cannot be avoided.
- Many of the people approached responded to the questionnaires based on their moodand feelings at that moment of time.
- Time factor can be considered as a major limitation.
- As the study was done within a limited time, investigation could not select asufficiently large sample for the study.

4. SUGGESTIONS

- Managing cyber risks: Banks should consider building cyber risk management programs to achieve three essential capabilities: the ability to be secure, vigilant, andresilient.
- Being Secure: A good understanding of the known threats and controls, industry standards, and regulations can guide financial services firms to secure their systemsby design and implementation of preventative, risk-intelligent controls.
- Becoming vigilant: Banks' monitoring systems should work 24/7, with adequatesupport for efficient incident handling and remediation processes
- Install a dedicated, actively managed firewall. Use a regular operating system and keyapplication security patches

5. CONCLUSION

A banking organization is the key to economic growth and development of the country. Financial & social reforms were carried out in the banking sector in India after independence. Due to adoption of technology traditional banking shifted to electronic banking popularly known as e-banking. ATMs were introduced to the Indian banking industry in the early 1990s initiated by foreign banks and customers are now conversant withthe concept of banking 24x7 through ATMs. The implementation of new technology in banking industry and advancement of e-banking not only offered opportunities for the profitable development of banking business but has also pave the way for new criminal activities to take advantage of technology.

Adoption of technology in banking put a serious threat to the banking institutions known as "Cyber Crimes". The global nature of computer technology presents a challenge to nations to address Cyber-crime. Domestic solutions are inadequate because cyberspace has no geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. The internet is the medium for huge information and medium of communication around the world, it is necessary to take certain precautions while operating it. To prevent the cyber frauds, it is necessary to take certain precautions while operating the computer or internet. It is very important to educate every one and make them aware of cyber fraud and punishments penalties for safe surfing and browsing, make them aware how to use and handle mobile and online banking, how to secure personal information, how to use various applications, what precautions has to be taken while doing online banking transactions. It is necessary to strongenforcement of cyber-crimes rules and regulations.

6. BIBLIOGRAPHY JOURNALS

[1] Arora, S. s. (2020). Customers' usage behaviour of e-banking services: Interplay of electronicbanking

[2] and traditional banking. https://www.researchgate.net/. Douglas, L. a. (2000).

[3] Cybercrime Security and Surveillance in the Information Age. Routledge. Goodman, M. (2015). Future Crimes: How Our Radical Dependence on Technology Threatens Us All. Hussain, R. (2016). CYBER-CRIMES AND E-BANKING AN EMPIRICAL STUDY.

Websites

[4] https://www.academia.edu/. KARN, D. S. (2014). CYBER CRIME IN BANKING SECTOR.

[5] https://journal.lawmantra.co.in/. Neena, S. R. (2013). An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks.