International Journal of Advances in Business and Management Research (IJABMR)
https://ejournal.svgacademy.org/index.php/ijabmr/

https://doi.org/10.62674/ijabmr.2024.v2i02.002
OPEN ACCESS

THE DARK SIDE OF CASHLESS TRANSACTIONS: UNDERSTANDING THREATS TO BANKING SECURITY

Mehak[*], Shailinder Sekhon

Original Article

Punjabi University Patiala, NH 64, next to Urban Estate Phase II, Patiala, 147002 Punjab, India

*Corresponding Author's Email: mehak96.pbi@gmail.com

Abstract

The digital revolution is considered one of the most significant events in the course of human history. The exponential growth in the usage of the Internet, e-commerce, and mobile commerce has transformed the conduct of business. Similarly, the banking industry has experienced exponential growth as a result of the revolution in information technology. People without access to financial services now have more options to engage with and make direct use of banking services because of internet connectivity and mobile phones. Computers and other electronic media conduct all financial transactions nowadays. In order to use the internet's strength and keep up with the rapidly evolving business landscape, banks have established themselves on the Web. The digitalization of the banking sector has also led to an increase in the number of digital frauds in the country. Fraudsters and criminals have targeted cashless banking as a means to steal personal information from customers. Although cashless banking has improved bank efficiency and made people's lives easier, it also raises the danger of fraud and other risks. This study highlights the numerous risks that customers face when using cashless banking.

Keywords: Cashless Banking; Cybercrimes; Digital; Frauds; Technology; Threats

Introduction

The increasing prevalence of smartphones and internet access has changed the options available to consumers when it comes to interacting digitally for online shopping, information sharing, and money transfers. Now-banked individuals can also directly utilize financial services thanks to mobile banking and the internet [1]. Financial institutions are also interested in technological advances, such as the internet and mobile banking, electronic money transfers, crypto-currencies, and interbank financial telephony, in order to strengthen and improve the effectiveness of the modern financial system [2].

Using ATMs, debit/credit cards, POS terminals, cheques, or mobile phones and the internet, cashless banking settles transactions electronically without the need for cash [3]. Other names for cashless banking include e-banking, mobile banking, internet banking, and online banking, among others. Both the customers and the banks have benefitted from cashless banking. The Internet has helped banks reduce their operating expenses by allowing them to have fewer physical locations for staffing, documentation, and personnel. By just clicking on smartphones or PCs with internet

Received 4th October 2024; Revised 15th October 2024; Accepted 11th November 2024

connectivity, customers may also access a wide range of financial services, including paying utility bills, transferring money from one place to another, making balance requests, applying for loans, and more. Even though banks offer their clients advantageous online services, the practice of cashless banking has raised several security concerns [4]. Computer hackers have devised numerous cunning techniques to pilfer customers' funds. Cashless banking has numerous benefits, but security concerns, privacy, and fraud sometimes deter users from adopting it, as they fear that using it might jeopardize their investments. Cybercriminals utilize advanced technology and devices to breach bank accounts, and they employ malware, phishing, viruses, Trojans, spoofing, identity theft, and pharming to perpetrate cashless banking frauds.

Statement of the Problem

Financial organizations may make significant profits through cashless banking. Customers may pay bills, transfer money, and obtain important information online with ease and flexibility thanks to it. Online fraudsters and criminals seeking to steal consumer information are currently posing serious hurdles due to the hazards of fraud, security risk, and malware attacks. The decline in cashless banking usage and the erosion of customer trust in financial institutions' security measures are both results of the surge in cyberattacks. Customers are looking to banks to address their concerns about the security of their money and information. Therefore, this study highlighted the numerous risks and threats that customers face when using cashless banking and provided some suggestions to mitigate these frauds or crimes.

Research Methodology

The study is based on secondary data that has been collected from various secondary sources such as magazines, newspapers, research papers, blogs, etc. Moreover, to find the relevant literature, some keywords like threats to digital banking, online frauds, and cybercrimes were used to search the research papers on different websites like Google Scholar, JSTOR, Science Direct, and Emerald Insight.

Literature Review

Threats of Cashless Banking

When there is a new technology or invention, it can be both beneficial and harmful for society, but it mainly depends on how a person uses it. While the majority of individuals use computers for positive, morally responsible purposes, others use them for harmful, immoral, or unlawful purposes. Likewise, computer crime has a long history dating back as far as computers. Fraud may be classified as "Computer Crime" if it is carried out via a computer [5]. It is a breeze for a criminal to conduct an illicit operation with the help of the internet. Cybercrime refers to any online or internet-based criminal activity. Cybercrime encompasses both traditional criminal activity and newly developed activities resulting from the development of new media platforms. Cybercrime can encompass any behavior that essentially violates human sensibility.

- ***Phishing***

  Phishing, a growing menace in the online world, is primarily due to advancements in technology and social networking. In the phishing method, the perpetrator employs social engineering techniques to steal an individual's identity [6]. Phishing typically involves sending out forged emails that imitate an online bank, meticulously crafted to resemble the login to the real site [4]. Phishing uses the persona of a reputable online company to get private and sensitive data, including credit card details, usernames, passwords, and even cash [7].

- ***Trojans***

  Trojans are a type of malware that poses as a reliable source, deceiving the user into taking actions that result in the installation of the malware on their device. Malicious code-infected websites or simple attachment downloads from emails can also facilitate this installation. Trojan horses frequently create backdoor-hidden openings, enabling unauthorized users to remotely access compromised computer systems and circumvent security measures [8].

- ***Spoofing***

The act of a cybercriminal impersonating a reliable source or tool in order to trick you into doing something that would benefit the hacker but harm you is known as "spoofing." Spoofing is the practice of internet scammers disguising their identity as someone else. Spoofing comes in various forms, such as spoof emails, IP spoofing, DNS spoofing, GPS spoofing, and website spoofing [9].

With the intention of obtaining information, demanding ransom, or infecting the device with malware or other dangerous software, the adversary can then interact with the target and get access to their systems or devices.

- ***Computer virus***

Clicking on a link or attachment in an email or downloading any software can infect the computer or mobile device with malware or malicious software. Hackers may be able to access our bank account details or financial information through a virus without the user's awareness.

- ***Hacking***

Using a variety of methods to take advantage of weaknesses in computer networks, websites, or systems is what hacking generally entails. Hackers search for vulnerabilities and find points of access to the system using a variety of instruments and software [5]. They could attempt to steal confidential information, disrupt financial transactions, or harm the system in other ways once they get access. Hackers typically use this method to gain unauthorized access to computer networks and systems [1].

- ***SMiShing***

SMiShing, a type of phishing technique that targets mobile devices, uses short messaging services, or SMS, in place of phone calls or email. The term "SMiShing" comes from SMS (Short Message Service) text messaging. The two basic stages of a SMiShing scam are as follows: Initially, the scam appears as communication from your acquaintance or bank, while the subsequent phase involves receiving a crucial text message alerting you to theft of your identity or the locking of your account number. It then provides you with a phone number or website to verify the account details. The criminals take money out of the account or apply for a new credit card in the victim's name after obtaining the details [10].

- ***Vishing***

Phishing and vishing are quite similar, except instead of using emails to trick victims into divulging personal information, fraudsters use phone calls (either recorded or live) called "robocalls." Often, criminals rely on impersonating a nearby bank, credit union, or company that you might be tempted to trust or do business with and ask for your personal or confidential information [10].

- ***Cookies***

Phishing and vishing are quite similar, except instead of using emails to trick victims into divulging personal information, fraudsters use phone calls (either recorded or live) called "robocalls." Criminals frequently impersonate a nearby bank, credit union, or company that you might be inclined to trust or conduct business with, requesting your personal or confidential information. Cookies, which are small text files downloaded to a user's computer when accessing a website, store the information that the website server transmits to the user's browser. A web user may occasionally be able to examine cookies in the header source code of a webpage if they so want. On the other hand, the user's computer and browser often record, track, and retain the information instead of displaying it to them. The user's web browser will send the previously stored data to the website upon their return. Through the surveillance of certain computers' movements, cookies enable websites to identify a machine that was present a while ago [5]. These cookies record a person's data, potentially enabling hackers to obtain personal information and engage in illegal activities [10].

- ***Salami slicing attack***

  According to the Oxford Dictionary, "salami-slicing" is the act of making something smaller over time by making small, incremental changes to its size. Such an attack will have such a minor effect that none of the victims will notice it individually; collectively, the effect is enormous. The slicing strategy encompasses personal data gathered from various sources, such as online surveys, deposit sites that gather trash information, documents that have been borrowed or stolen, targets' banking transaction details, contact information, and whereabouts [11]. These sources offer a plethora of factual information about the individual, ideal for fraudulent activities such as defamation and forgery.

Suggestions for Mitigating Bank Fraud

- It is advantageous to continuously monitor all SMS or emails that appear while conducting any type of transaction.
- It is advised to purchase goods from reliable and certified retailers only because the reputed website is trustworthy and secure.
- It is imperative that you never divulge private information to anybody, not even those who seem like bank representatives or independent mobile app developers, including your credit/debit card number, CVV number, or OTP (one-time password).
- It is recommended that all PCs and gadgets have antivirus, firewall, and other security software installed. Additionally, avoid charging your computers or cell phones in public areas such as railway stations, airports, etc.
- Make sure your password is strong and has a combination of capital and lowercase letters, numbers, and special characters. It should be at least eight characters long and keep changing your passwords frequently.
- Be vigilant against phishing scams, which trick users into revealing sensitive information through emails and websites. Avoid clicking on links and attachments and popping up windows from sources you do not trust.
- Maintaining the privacy of your personal information is important since hackers can use your social media accounts to decipher passwords and provide answers to security questions in password reset programs.
- Monitor your credit report and bank documents closely to prevent identity theft. To prevent payback requests for loans you never took out, report any unauthorized loans to your bank and credit bureaus as soon as possible.

Discussion

The increasing reliance on digital platforms for financial transactions has made cashless banking an attractive target for cybercriminals. There were 6583 registered cybercrime cases in India in 2022, highlighting a growing trend of online fraud that threatens consumer confidence in cashless banking [12]. As individuals engage more frequently with online banking and e-commerce, they become more vulnerable to sophisticated cyberattacks [1]. Some threats like phishing, malware, spoofing, SMiShing, vishing, etc. have led to a significant erosion of consumer trust in the cashless banking system. Many individuals are hesitant to adopt digital payment solutions due to fears of fraud and identity theft [13]. This skepticism not only hinders the growth of digital banking services but also limits financial inclusion efforts aimed at underserved populations [1]. Artificial intelligence is proving to be an invaluable asset in the fight against cybercrime in the banking sector. By enhancing fraud detection capabilities, improving security measures through biometrics, facilitating automated responses, detecting phishing attempts, and enabling effective risk assessment, AI is helping banks protect their customers and maintain trust in digital financial services [14]. However, on-going vigilance is necessary to address the challenges associated with AI implementation and ensure that these technologies continue to evolve alongside emerging threats [15]. By implementing comprehensive security measures and fostering consumer awareness, the banking sector can enhance trust and ensure a safer digital transaction environment. As technology continues to evolve, on-going vigilance against cyber threats will be critical in maintaining the integrity of cashless transactions.

Conclusion

In conclusion, cashless banking has transformed the financial landscape, offering numerous advantages such as enhanced convenience, reduced operational costs, and increased accessibility. The widespread use of mobile banking, e-commerce, and other digital platforms has made financial services more efficient and accessible to a larger population. However, alongside these benefits, the proliferation of cashless transactions has also introduced significant risks. Cybercrimes, including phishing, Trojans, spoofing, and hacking, have become more prevalent, posing serious threats to the security and privacy of users. Hackers employ sophisticated techniques to access sensitive information, making users vulnerable to identity theft, financial fraud, and data breaches.

The increase in digital fraud has raised concerns among customers, leading to a decline in trust in online banking systems. The complexity and evolving nature of cyber threats, which often remain undetected until significant damage has occurred, exacerbate this distrust. Despite banks implementing advanced security measures such as firewalls, encryption, and multi-factor authentication, these efforts alone cannot entirely eliminate the risks. Users must also remain vigilant by adopting safe online practices, such as creating strong passwords, avoiding suspicious emails or links, and monitoring their financial accounts regularly.

To ensure the sustainability and continued growth of cashless banking, a collaborative approach is essential. Financial institutions must invest in more advanced cyber-security solutions, while users must stay informed about the latest threats and adopt preventive measures. Furthermore, governments and regulatory bodies need to implement stringent policies to protect consumers from cybercrimes. Only through collective efforts can the full potential of cashless banking be realised without compromising the security and privacy of users. Ultimately, the future of cashless banking depends on creating a secure digital environment that fosters trust and confidence among all stakeholders.

Conflict of Interests

The authors declare that they have no conflict of interests.

Acknowledgement

The authors are thankful to the institutional authority for completion of the work.

References

1. Saluja S, Nair AJ. An Analysis on Frauds Affecting the Financial Security of the Indian Banking Sector: A Systematic Literature Review. Ethical Marketing Through Data Governance Standards and Effective Technology. 2024:201-18. http://dx.doi.org/10.4018/979-8-3693-2215-4.ch017

2. Wonglimpiyarat J. FinTech banking industry: a systemic approach. foresight. 2017 Nov 13;19(6):590-603. https://doi.org/10.1108/FS-07-2017-0026

3. Yazdanifard R, WanYusoff WF, Behora AC, Sade AB. Electronic banking fraud: The need to enhance security and customer trust in online banking. Advances in Information Sciences and Service Sciences. 2011;3(10):505-9. http://dx.doi.org/10.4156/aiss.vol3.issue10.61

4. Alsayed A, Bilgrami A. E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. International Journal of Emerging Technology and advanced engineering. 2017 Jan;7(1):109-15.

5. Kaur DG. Threats to the rights of consumers in E-banking in India: An overview. Available at SSRN 2983199. 2017 Jun 8. Kaur, Gagandeep, Threats to the Rights of Consumers in E-Banking in India: An Overview (June 8, 2017). http://dx.doi.org/10.2139/ssrn.2983199

6. Khonji M, Iraqi Y, Jones A. Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials. 2013 Apr 15;15(4):2091-121. https://doi.org/10.1109/SURV.2013.032213.00009

7. Aleroud A, Zhou L. Phishing environments, techniques, and countermeasures: A survey. Computers & Security. 2017 Jul 1;68:160-96. https://doi.org/10.1016/j.cose.2017.04.006

8. Vaciago G, Ramalho DS. Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. Digital Evidence & Elec. Signature L. Rev. 2016;13:88. https://doi.org/10.14296/deeslr.v13i0.2299

9. Schuckers SA. Spoofing and anti-spoofing measures. Information Security technical report. 2002 Dec 1;7(4):56-62. https://doi.org/10.1016/S1363-4127(02)00407-7

10. Blancaflor E, Romero MA, Nacu I, Golosinda DR. A Case Study on Smishing: An Assessment of Threats against Mobile Devices. InProceedings of the 2023 9th International Conference on Computer Technology Applications 2023 May 10 (pp. 172-178). https://doi.org/10.1145/3605423.3605446

11. B., Tapasya. The Aspects of Probing into the Online Fraud of'Salami Slicing Attack'. Part 1 Indian J. Integrated Rsch. L.. 2022;2:1.

12. Hazra D. What does (and does not) affect crime in India?. International Journal of Social Economics. 2020 Apr 16;47(4):503-21. https://doi.org/10.1108/IJSE-03-2019-0206

13. Abdullah SM, Ahmed B, Ameen M. A new taxonomy of mobile banking threats, attacks and user vulnerabilities. Eurasian Journal of Science and Engineering. 2018 Jun 1;3(3):12-20. https://doi.org/10.23918/eajse.v3i3p12

14. Ghandour A. Opportunities and challenges of artificial intelligence in banking: Systematic literature review. TEM Journal. 2021;10(4):1581-7. http://dx.doi.org/10.18421/TEM104-12

15. AL-Dosari K, Fetais N, Kucukvar M. Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. Cybernetics and systems. 2024 Feb 17;55(2):302-30. https://doi.org/10.1080/01969722.2022.2112539

16. Featherman MS, Pavlou PA. Predicting e-services adoption: a perceived risk facets perspective. International journal of human-computer studies. 2003 Oct 1;59(4):451-74. https://doi.org/10.1016/S1071-5819(03)00111-3

17. Kamalul Ariffin S, Mohan T, Goh YN. Influence of consumers' perceived risk on consumers' online purchase intention. Journal of research in Interactive Marketing. 2018 Oct 16;12(3):309-27. https://doi.org/10.1108/JRIM-11-2017-0100

18. Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PK, Singh S. A review on cyber crimes on the internet of things. Deep Learning for Security and Privacy Preservation in IoT. 2022 Apr 4:83-98. https://doi.org/10.1007/978-981-16-6186-0_4

19. Omariba ZB, Masese NB, Wanyembi G. Security and privacy of electronic banking. International Journal of Computer Science Issues (IJCSI). 2012 Jul 1;9(4):432.