e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

TRUST & SECURITY ISSUES IN MOBILE BANKING AND ITS EFFECT ON CUSTOMERS

Balachandra Rao*1, Shashank Ganesh Suvarna*2

*1,2Nitte Deemed to be University, Department of MCA, NMAM Institute of Technology, Nitte, Karnataka, India.

balachandra22@nitte.edu.in

shashankganesh53@gmail.com

DOI : https://www.doi.org/10.56726/IRJMETS39238

ABSTRACT

Mobile banking has revolutionized the way people manage their finances. However, the convenience of accessing bank accounts through mobile devices also brings security risks. Cybercriminals can gain unauthorized access to mobile phones, intercept personal information, and conduct fraudulent transactions. This has become a major concern for banks and customers alike. This summary outlines the risk of using mobile devices for payments as well as precautions that can be implemented. It discusses the various types of mobile banking frauds, such as phishing, malware attacks, and SIM swapping. The paper also covers the security measures that banks can implement, such as two-factor authentication, biometric authentication, and real-time fraud monitoring. Finally, the abstract emphasizes the importance of customer education and awareness about safe mobile banking practices. Overall, the paper provides insights into the challenges and solutions for securing mobile banking transactions.

Keywords: Mobile banking, transactions , Malware , Phishing attacks , Insider threats , two-factor authentication .

I. INTRODUCTION

The widespread adoption of mobile phones has transformed the way we interact with the world around us, including how we manage our finances. With the rise of mobile banking, consumers can now access their bank accounts, make payments, and conduct transactions from the palm of their hand. While this has brought unparalleled convenience, it has also brought new security risks. Cybercriminals are exploiting vulnerabilities in mobile devices to gain unauthorized access to bank accounts, intercept personal information, and carry out fraudulent transactions. As a result, the threat of accessing mobile phones for bank transactions has become a major concern for both banks and their customers. This paper examines the various types of mobile banking frauds, the security measures that banks can implement, and the importance of customer education and awareness. The goal is to provide insights into the challenges and solutions for securing mobile banking transactions and to highlight the need for a collaborative approach to mitigating these risks.

II. LITERATURE REVIEW

There is still a lot of room for advancement in mobile banking operations and services such account transfers, balance enquiries, bill payments, stop-payment requests, and some even offer online loan and credit card applications. Therefore, it is important to comprehend user acceptance of mobile banking and pinpoint the variables driving users' inclinations to use mobile banking[1]. Mobile payment is becoming more commonplace as mobile the organisation expands quickly. Although there is a plethora of academic research on mobile payments, there are no uniform standards for both physical and virtual mobile payments, and the current mobile payment procedures lack trust mechanisms. Furthermore, it is challenging to connect applications with banks given the present mobile payment patterns. This study offers a new mobile payment pattern that promotes layered extension and cascading agent based on stable and reliable platform group to address this issue. It also provides a basic framework for online mobile payment. Additionally, it suggests a cross-bank unified payment platform to address the problems with bank connections[2]. Because it is SMS-based, the m-payment (mobile payment) transaction model between the consumer and the merchant in m-commerce (mobile commerce) is simple for payment at any time and anyplace. Advanced mobile phones are not required, and third-party payment gateways do not impose additional fees. For small consumers and small business owners using bank transactions, this strategy is particularly advantageous. Biometrics can be used to improve

security. Simply put, this is a model. For completing secure m-payment transactions, hardware-side security measures are quite potent[3]. The authors came to the conclusion that by embedding a biometric finger-print method, only authorised users would be able to utilise mobile banking services. It was discovered through a survey of the literature and interviews that the finger-print mechanism is more appropriate than other typical systems like the login and password system, SMS, etc [4]. The performance of four e-payment systems—the credit card, the stored-value card, the smart card, and the telecommunication bill—is assessed in this study using the analytic hierarchy process (AHP), a quantitative approach of decision-making. The outcomes indicate that, of the four solutions taken into consideration, the stored-value card performs the best. Our findings also imply that despite a payment option's technical imperfections like a credit card, it may nevertheless end up being the de facto e-payment method because of the benefit of an established client base. This leads us to propose that, in order for e-payment systems with better economic/social merits to establish a vital customer base, additional usages be added. The widespread utilisation of technologically advanced e-payments for internet business will benefit users [5].

III. CYBER SECURITY RISK SCENARIOS

There are a variety of cyber security risk scenarios that individuals and organizations should be aware of. Here are some examples:

1. Phishing attacks :A typical threat to cyber security situation is a phishing scam, when an intruder delivers a text or email that looks to be from a reliable source in an effort to deceive the receiver into disclosing private information like passwords for accounts, banking details, or personal data.

2. Ransomware: A form of virus known as ransomware encodes data belonging to an organisation, rendering it useless unless the hacker is paid a ransom. The operation and repute of an organisation may suffer as a result.

3. Social engineering: The practise of social engineering is the practise of using emotional deception to coerce people into disclosing confidential information or taking activities that could compromise the security of an organisation. Tactics used in the practise of social engineering include baiting, tailgating, and pretexting.

4. Insider threats: Insider threats happen when staff members or contractors with access to a company's systems or data abuse their privileges, either purposefully or accidentally jeopardising the security of the company.

5. Distributed Denial of Service (DDoS) attacks: DDoS attacks involve overwhelming an organization's servers with traffic, rendering them unavailable to legitimate users. This can be used as a tool for extortion, as the attacker may demand payment to stop the attack.

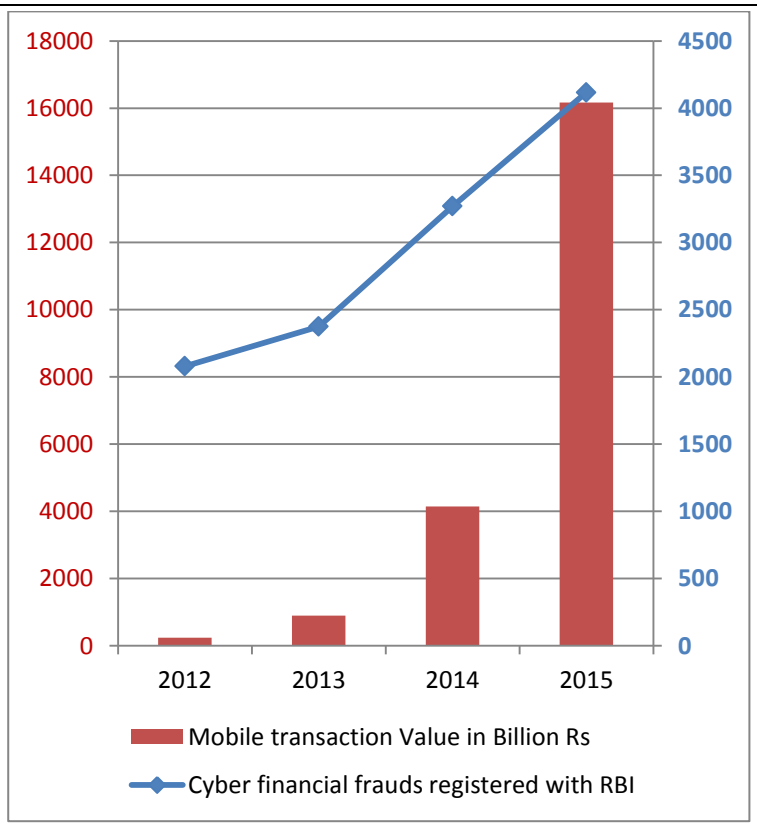
6. Advanced persistent threats (APTs): Nation-states or organised crime groups frequently conduct APTs, a specific kind of cyberattack. These assaults aim to get continuous access to a the company's systems or information and are extremely advanced, frequently involving numerous stages.

7. Malware: Any software that is designed to cause damage to the systems of an organization or data is known as malware. Malware often arrives in the nature of viruses, worms, and trojans..

8. Supply chain attacks: Supply chain attacks involve targeting a vendor or supplier of an organization's software or hardware, with the goal of infecting the organization's systems through a trusted source. This can be difficult to detect and mitigate, as the attack may not originate within the organization itself.

Overall, these cyber security risk scenarios show how crucial it is to take proactive steps to safeguard against potential dangers. This involves putting in place robust security safeguards like multi-factor authentication, frequent software updates, and employee training on cyber security standards.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com



Over time, there have been more and more cases of credit and debit card fraud. Based on NCRB data, Maharashtra, Uttar Pradesh, Karnataka, and Andhra Pradesh are among the States with the highest incidences of cybercrime. Incidentally, Compared to the other States, these States have more internet users.

Negative impact of cyber fraud

Cyber fraud can have a variety of negative impacts on individuals, companies, and society at large. Here are a few scenarios:

1. Financial losses: Cyber fraud can result in significant financial losses for individuals and organizations. This includes unauthorized access to bank accounts, credit card fraud, and fraudulent wire transfers.

2. Reputational damage: Cyber fraud can damage an organization's reputation, particularly if it involves the loss of sensitive data such as personal information or trade secrets. This can lead to a loss of customer trust and damage the organization's brand.

4. Legal and regulatory consequences :Legal and regulatory consequences from hacking might impact people and businesses. This include monetary penalties, legal proceedings, and the possibility of criminal prosecution for individuals responsible for the deceit.

4. Business disruption: Cyber fraud can also cause significant disruption to an organization's operations, particularly if critical systems are affected. This can result in downtime, lost productivity, and additional costs associated with recovering from the attack.

5. Psychological impact: Cyber fraud can also have a psychological impact on victims, particularly if sensitive personal or financial information is compromised. This can lead to feelings of anxiety, stress, and a loss of trust in online systems.

6. Economic impact: Cyber fraud can have a significant economic impact on society as a whole. This includes lost productivity, increased costs associated with cybersecurity measures, and reduced confidence in online systems, which can negatively impact e-commerce and other online businesses.

Overall, cyber fraud is a major risk and may have a variety of adverse consequences. Individuals and organisations must act actively to protect themselves from cyber fraud, such as putting in place robust cyber security measures and being on alert for fraud's warning data.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

IV. GENERAL CYBER SECURITY THREATS TO THE MOBILE DEVICE

Mobile devices, such as smartphones and tablets, are increasingly popular targets for cyber criminals. Here are some of the general cyber security threats to mobile devices:

1. Malware: Malware is malicious software that can infect a mobile device through a variety of means, such as malicious apps, phishing emails, or unsecured Wi-Fi networks. Malware can be used to steal personal information, track user activity, and take control of the device.

2. Phishing: Phishing attacks use fake login page or email to trick users into revealing information that is private, such login credentials or financial information. Phishing attacks can be difficult to spot as they often originate from which looks to be a reliable source.

3. Unsecured Wi-Fi networks: Public Wi-Fi networks, such those present at airports or coffee shops, can be subject to hacking efforts.. Users who connect to unsecured networks may be at risk of having their data intercepted by cyber criminals.

4. Physical theft or loss: Mobile devices can be lost or stolen, putting the data stored on them at risk. Cyber criminals may also be able to gain access to a lost or stolen device if it is not properly secured with a passcode or biometric authentication.

5. Outdated software: Outdated software, such as operating systems or apps, can contain vulnerabilities that cyber criminals can exploit to gain access to a device or steal data.

6. Fake apps: Fake apps that mimic legitimate apps, such as banking or social media apps, can be used to steal sensitive information or infect a device with malware.

7. Jailbreaking or rooting: Jailbreaking or rooting a mobile device can bypass security measures and allow users to install unauthorized apps or access restricted data. However, this also opens up the device to potential cyber attacks.

In overall, mobile devices are at risk of a range of cyber security risks. Users need to be proactive in maintaining their devices by using strong passwords, managing updated software, and keeping free of open Wi-Fi networks.

How to ensure safe Mobile Banking?

Mobile banking has become increasingly popular, but it also comes with potential risks. Here are some steps you can take to ensure safe mobile banking:

1. Only download programmes from legitimate sources, such as the official app stores, if your goal is to use mobile banking. Apps from unknown sources should be prohibited since they can be unsafe.

2. choose strong passwords: For your mobile banking app, choose a strong and distinctive password. Try to stay out of using passwords "1234" or "password".

3. Enable two-factor authentication: For your mobile banking app, enable two-factor authentication (2FA). By requiring a second authentication method, such as a fingerprint or SMS code, this ups security by a single level.

4. Keep your device up-to-date: Make sure your device is running the latest operating system and security updates. These updates often include security patches that can help protect against potential vulnerabilities.

5. Avoid public Wi-Fi:For mobile banking, stay out of using public Wi-Fi networks as they may be risky and open to hacking attempts. Use your mobile data instead, or a safe and dependable Wi-Fi network.

6. Keep an eye on your accounts: Be plans to keep an eye out for any odd activity in your bank accounts. As soon as you are notice of any illegal transactions, call your bank.

7. Log out after use: Always log out of your mobile banking app after use, and never leave your device unlocked or unattended.

By following these tips, you can help ensure safe mobile banking and protect your personal and financial information. It is important to stay vigilant and take proactive steps to protect against potential threats.

Advice for a safe mobile banking ecosystem

Here are some suggestions for a safe mobile banking ecosystem:

1. Robust authentication mechanisms: To make sure that authorised individuals have access to mobile banking services, use solid methods of authentication like biometric authentication or multi-factor authentication.

2. Encryption: Use encryption to protect sensitive data, such as login credentials and transaction information,

both during transit and at rest.

3. Regular security audits: -Conduct regular checks on security in order to spot any vulnerabilities in the mobile banking ecosystem and take steps needed to fix them.

4. Real-time fraud detection: Implement real-time fraud detection and prevention mechanisms to identify and prevent fraudulent transactions.

5. Secure communication channels: Use secure communication channels, such as HTTPS or SSL, to ensure that data is transmitted securely between the mobile banking app and the bank's servers.

6. Continuous monitoring: Continuously monitor the mobile banking ecosystem for potential threats, such as malware or phishing attacks, and take immediate action to mitigate any risks.

7. Customer education: Educate customers on safe mobile banking practices and provide them with resources, such as security tips and best practices, to help them protect their personal and financial information.

By implementing these measures, banks and financial institutions can help ensure a more secure mobile banking ecosystem and protect their customers' sensitive information. It is important to stay proactive and stay up-to-date with the latest security best practices to stay ahead of potential threats.

V. CONCLUSION

In conclusion, Trust and Security issues in mobile banking have a significant impact on customers' behavior and confidence in using these services. Customers are increasingly relying on mobile banking due to its convenience, accessibility, and efficiency. However, the growing use of mobile banking has also led to concerns about the security and privacy of personal and financial information. To address these concerns, mobile banking providers must prioritize the development and implementation of robust security measures such as multifactor authentication, encryption, and biometric identification. Furthermore, it is crucial for these providers to be transparent with their customers about the measures they have in place to protect their data. Customers must also take steps to ensure their own security, such as using strong passwords, avoiding public Wi-Fi networks, and regularly monitoring their accounts for suspicious activity. Ultimately, the success of mobile banking hinges on the establishment and maintenance of trust between providers and customers. By prioritizing security and transparency, mobile banking providers can build this trust and continue to grow their user base.

VI. REFERENCES

[1] Mohammed-issa R Jaradat, Naseem M Twaissi, “Assessing the Introduction of Mobile Banking in Jordan Using Technology Acceptance Model,” Jan. 2010, vol4,IJIM.

[2] Deli Yang, Hongxin Wang, Yawei Ren, and JianJun Wang, —Mobile Payment Pattern Based on Multiple Trusted Platforms - China Case,|| Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference on, 2010, pp. 353-362.

[3] P. Soni, —M-Payment Between Banks Using SMS [Point of View],|| Proceedings of the IEEE, vol. 98, 2010, pp. 903-905.

[4] Loretta Michaels,Forward, Dr. Allen L. Hammond, “Biometric Security for Mobile Banking” March.2008. White Paper.

[5] Y. Chou, C. Lee, and J. Chung, —Understanding m-commerce payment systems through the analytic hierarchy process,|| Journal of Business Research, vol. 57, Dec. 2004, pp. 1423-1430.