

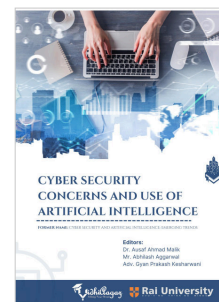
CHAPTER 27

Secure Transactions, Reliable Future: Unravelling the Complexities of Cybercrime in India's E-Banking Sphere

Asif Pasha and Milan Donson

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 226–232

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Asif Pasha & Milan Donson, *Secure Transactions, Reliable Future: Unravelling the Complexities of Cybercrime in India's E-Banking Sphere*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 226 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Asif Pasha and Milan Donson, 'Secure Transactions, Reliable Future: Unravelling the Complexities of Cybercrime in India's E-Banking Sphere' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 226.

CHICAGO (17TH ED.)

Pasha, Asif, and Milan Donson. "Secure Transactions, Reliable Future: Unravelling the Complexities of Cybercrime in India's E-Banking Sphere." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 226–232. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-27/>.

APA (7TH ED.)

Pasha, A., & Donson, M. (2024). Secure transactions, reliable future: Unravelling the complexities of cybercrime in India's e-banking sphere. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 226–232). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-27/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-27/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

SECURE TRANSACTIONS, RELIABLE FUTURE: UNRAVELLING THE COMPLEXITIES OF CYBERCRIME IN INDIA'S E-BANKING SPHERE

Asif Pasha³⁷ and Milan Donson³⁸

ABSTRACT

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

—Newton Lee

The Internet, an intricate global network of interconnected devices, functions as a medium for the exchange of information and connectivity. However, it also harbours a darker side, serving as a platform for 'cybercrime', illicit activities that exploit this technology to gain unauthorized access to data or systems that can target crowds at large, leading to extraordinary losses and hopeless situations. It manifests in various forms and is often transnational and anonymous which complicates the process of identification, tracking, and prosecution of the perpetrators. The e-banking sector is particularly susceptible to cybercrime because transactions often involve third parties, providing cybercriminals with opportunities to interfere unapproved posing a significant challenge not only to technological advancement but also to the protection of individual privacy. In India, traditional banking methods are being rapidly supplanted by e-banking. The transition from conventional crime to cybercrime is both novel and sophisticated since cybercriminals can operate under the veil of anonymity. As economic factors lead to an increase in the amount of money deposited, there is a growing trend towards the use of electronic methods for money storage and transfer. This trend necessitates vigilant monitoring to prevent potential cybercrimes.

Keywords: Cyber Crime, Cyber Terrorism, E-Banking, Technology, Internet.

INTRODUCTION

The world economy has derived into a new scenario of development, courtesy of cutting the Red Tape when our country woke up from its slumber in the most stringent of hours. The Internet revolution has brought the world economy to a new level of advancement. These changes made people advance in every area of life.

Today, the Internet has become an integral part of our daily life. In 2021, there were about 4.66 billion active internet users worldwide, which is about 59.5 percent of the global population. In 2023, India had the second-highest number of internet users in the world, with about 692 million users, which is about half of its population. The Internet accounted for 21 per cent of the GDP growth in mature economies over the past 5 years. Technology has also changed how and where we consume media, how we communicate, and how we tackle global challenges.

RESEARCH QUESTION

- What are the main types and causes of cybercrime in India, and how do they affect the e-banking sector?
- What are the best practices and strategies to enhance the security and privacy of e-banking

³⁷ Student at Kristu Jayanti College of Law, Bangalore, India.

³⁸ Student at Kristu Jayanti College of Law, Bangalore, India.

customers and service providers in India?

OBJECTIVE

To analyse the nature, causes, and impacts of cybercrime and cyber terrorism in India, and to evaluate the existing and potential solutions to prevent and combat them in the context of e-banking.

METHODOLOGY

This research utilizes secondary data from diverse sources, including official data, books, articles, journals, reports, magazines, newspapers, and websites, to analyse the evolution of banking and e-banking. Qualitative methods such as content analysis, thematic analysis, and comparative analysis are employed to examine the data. The paper also analyses regulations and their outcomes in combating cybercrime and cyberterrorism in the context of e-banking. The findings are interpreted to identify trends, challenges, and opportunities, and provide recommendations for enhancing security measures and regulatory frameworks in the e-banking sector.

E-BANKING

One of the most important aspects of our life that has been transformed by the Internet is money which allows us to manage our money anytime, anywhere, without any hassle and uses the Internet as a platform to deliver various services to customers. It has many benefits for both banks and customers, such as lower operational costs, higher convenience, faster transactions, and easier access to information.

The advent of digital payments and online banking, which are subsets of E-banking, has transformed the banking sector in India. The demonetization period in 2016 gave a boost to the adoption of digital payments, which were initially promoted by international banks. E-banking involves various types of digital payment methods, such as banking cards, mobile wallets, UPI, and AEPS, which have different features and benefits for users. It offers various benefits such as fund transfers, bill payments, deposits, account statements, and product orders.

People prioritize their comfort over the potential consequences they might face in the future. During the COVID-19 pandemic, internet banking became an integral part of daily life in India. It has become an advantage for many working in the online banking sector, as e-banking provides a safe way to conduct transactions such as paying bills and fund transfers. This trend is not likely to decrease anytime soon. Internet banking has revolutionized the way we manage our finances. As a result, it offers convenience, simplicity and efficiency in our daily lives. For example, we can access our accounts, transfer money, pay bills and check statements online anytime and anywhere. Therefore, banks use electronic media to provide a wide range of services that save time and resources.

Internet transactions have become a major mode of trading and individual transactions in the country, offering the cheapest way of providing banking services. However, e-banking services also entail risks along with benefits. For instance, they may expose customers to cyberattacks, frauds, or technical glitches. Despite these challenges, e-banking enhances the speed and convenience of transactions and

makes life simpler and happier. As more people join the net, the risks and opportunities of e-banking will also grow. Therefore, this problem needs to be addressed to ensure the future of net banking.

With a variety of options ranging from e-banking to mobile wallets, Asia is transforming the way people pay and get paid and is a pioneer in the field of digital payment solutions, having embraced them for almost a decade now. While Visa leads the E-Banking market, it faces tough competition from mobile payment options which is only poised to grow in the years to come.

While China, Korea, Japan and the SEA region were after this trend, with the introduction of a Uniform Payment Interface (UPI), India's dream of a cashless digital economy gained traction. UPI was adopted fairly quickly by the masses as a healthy consequence of events like overnight Demonetization which was further propelled by the Coronavirus Pandemic, which encouraged people to incorporate digital technology into their daily lives. As a result, digital payment has become a key mode of E-Banking for many Indians, although cash is still the king, it could soon be dethroned.

However, E-banking also comes with many challenges in the modern world. Despite the rules and security measures in place, it is not immune to cyber threats and risks, such as cybercrimes, security breaches, technical glitches, and customer dissatisfaction. Therefore, e-banking requires careful management and regulation to ensure its safety and reliability. Although E-banking is a convenient and cost-efficient way of accessing banking services through the Internet, it also has some drawbacks that may discourage some customers from using it.

CYBERCRIME

Internet transactions have become a popular way of conducting financial transactions, providing a cost-effective alternative to traditional banking services. However, the convenience of e-banking comes with certain risks, such as cyberattacks, frauds, and technical glitches. Despite these challenges, e-banking has made transactions faster and more convenient, simplifying people's lives. As more people adopt e-banking, the risks and benefits will continue to evolve, requiring ongoing attention to ensure the future of this mode of banking.

These cybercrimes are carried out by hackers who breach computer networks or systems to manipulate, steal, or destroy data, disrupt services, or take over the system. They may target individuals, businesses, or government entities for various motives, such as financial gain, political agenda, personal vendetta, or thrill-seeking. These cybercrimes violate the rights and dignity and expose to physical and mental harm. Specialized law enforcement units are working to prevent and prosecute these horrific crimes.

Security is the main concern and challenge of net banking. However, if proper safety measures are adopted, this issue can be resolved. For example, some banks have come up with innovative solutions to enhance the security level at every stage of the transaction, such as virtual keyboards and new grid-based debit cards.

To address the risk factors and challenges of online banking, RBI has issued guidelines to all banking institutions, advising them to take necessary steps to control this section of online banking. Moreover, the central government/RBI has made various provisions to solve the problem in banking sectors, such

as recruiting young and capable recruits who have specialized knowledge in the field of technology. The growth of Internet banking has also prompted many to rethink their information technology strategies in the competitive market.

The Reserve Bank of India (RBI) has issued several guidelines to ensure the security of financial transactions.

- Firstly never share account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM / Debit card / credit card details with anyone, even bank officials.
- Secondly, be cautious of any phone call or email threatening the blocking of account due to non-updation of KYC. Always access the official website of the bank or contact the branch for any updates.
- Avoid downloading unknown apps as they may secretly access confidential data.
- Remember that transactions involving receipt of money do not require scanning barcodes or entering MPIN.
- Always access the official website of the respective bank for contact details and to be wary of fraudulent contact numbers on internet search engines.
- Check URLs and domain names received in emails or SMSs for spelling errors and use only verified, secured, and trusted websites for online banking.
- If you receive an OTP for a transaction not initiated by you or a debit SMS for a transaction not done, inform your bank immediately.
- Do not share the password of your email linked to your bank account and avoid having common passwords for e-commerce or social media sites and your bank account.
- Do not set your email password as the word “password” or something very simple while registering on any website or application with email as user-id.
- Be wary of misleading advice intimating deposit of money on your behalf with RBI for foreign remittances, receipt of commission, or wins of lottery.
- Regularly check the email and phone messages for alerts from your financial service provider and report any unauthorized transaction observed to bank immediately.
- Lastly, secure your cards and set daily limit for transactions. You may also set limits and activate or deactivate for domestic or international use.

Fiscal fraud is a form of cybercrime that involves illegally obtaining confidential financial information. Some examples are:

- Credit card fraud: Using someone else's credit card details to make unauthorized purchases or withdrawals.
- Identity theft: Stealing someone's personal information, such as name, date of birth, or social security number, to open accounts, apply for loans, or commit other crimes in their name.

- **Phishing schemes:** Sending fraudulent emails or messages that appear to be from legitimate sources, such as banks, companies, or government agencies, to trick recipients into revealing their passwords, account numbers, or other sensitive data.
- **Online banking fraud:** Accessing someone's online banking account without their permission and transferring funds, paying bills, or changing settings.

These cybercrimes can have negative impacts on the e-banking sector, such as:

- Loss of customer trust and confidence in the security and reliability of e-banking services.
- Financial losses due to unauthorized transactions, refunds, or compensations.
- Legal liabilities and reputational damage due to data breaches or compliance violations.
- Operational disruptions or downtime due to cyberattacks or system failures.
- Increased costs for cybersecurity measures, insurance, or recovery efforts.

India is one of the top countries with the usage of the Internet. People in the country are compelled to use Internet services due to certain situations. E-banking in India has a bright future. There are many opportunities in e-banking. So, there will be a situation of misusing it. So, people who are using internet services like banking, e-commerce etc. should be aware of the privacy and security provided by the network. The negative side of net banking has become a challenge for the future. There should be proper rules and awareness of e-banking. If anything happens that is not accepted by the services, try to inform the consent authorities as soon as possible.

SUGGESTIONS

The existing rules are not sufficient to protect crores of people in the country from fraudulent activities in online banking. Internet Banking in India needs effective support to build the infrastructure for secure banking. The technical issues are still a threat to the security of Internet Banking. Tampering the websites and making fake websites all these issues will make the environment insecure. The hosting sector should itself need to focus on demonstrating and giving methods for the effective and secure use of online banking.

The study revealed that there is no way to completely eradicate cybercrime in the financial industry. Yet by assuring some fundamental security incentives from the bank to promote criminal activity in the approaching automated environment, it can limit its spillovers.

- **Better Authentication Techniques:** Banking institutions should investigate and use sophisticated authentication techniques that go beyond conventional passwords and 2FA. This could use behavioural analytics that examine user behaviours to find abnormalities or biometric authentication methods (like fingerprint or face recognition).
- **Continued Improvement of Encryption Protocols:** To safeguard sensitive data while it is being sent, online banking systems employ encryption techniques that are constantly improved. To keep ahead of new threats, use encryption algorithms that are industry standard and guarantee that they are updated often. Constant Monitoring and Fraud Detection Invest in

reliable monitoring solutions that can spot shady activity in real time. Use machine learning and artificial intelligence techniques to spot trends of fraud and proactively halt unlawful transactions.

- **Multi-Layer Security:** Put into practice a multi-layered security strategy that consists of firewalls, intrusion detection systems, and anti-malware programs. Perform routine security audits and penetration tests to find weaknesses in the net banking infrastructure. Address any flaws immediately, and ensure security fixes and upgrades are deployed often.
- **Customer Awareness:** Financial institutions should give client education and awareness campaigns top priority. Inform clients often about security best practices, typical risks, and how to keep secure when using online banking services. Users may benefit from this by learning more and taking greater initiative to safeguard their accounts.
- **Collaboration Efforts:** Encourage cooperation between banks, industry regulators, and cybersecurity specialists to exchange knowledge about new risks and effective practices. Rapider response times and more potent mitigation measures may result from this coordinated approach.
- **Regulatory Framework:** For online banking, governments and regulatory agencies should create and enforce strict security standards and laws. To secure consumer data, financial institutions must maintain a high degree of security and use standardised procedures.
- **Incident Response and Customer Support:** To handle security problems quickly, create a detailed incident response strategy and a dedicated customer support system. Be sure to promptly resolve any security-related concerns and provide clients with clear advice on how to report any suspicious activity.
- **Ongoing Security Training:** Inform bank staff members and employees regularly about the newest security risks, social engineering strategies, and best practices for protecting client data. Banks may lessen the risk of internal security breaches by retaining an informed and security-conscious workforce.

Internet banking is the cheapest way of providing banking. Internet banking is increasing, and it has become a “need to have” than a “nice to have” service. But there is still some traditional system in banking like cheque, cash withdrawals, etc. The digital world promotes digital services. The rules and laws will not provide complete protection. The awareness of society and individuals about the pros and cons of Internet banking is the basic importance.

CONCLUSION

The internet is a web of wonder that can bring us many benefits and opportunities. But it is also a web of woe that can expose us to many harms and hazards. We need to be careful and responsible when we use the internet and not let cybercriminals ruin our online experience. The main challenge is security and privacy. Even though there are security measures issued by the bank authorities, they are not helpful in the future. The main step that everyone can take is that be aware of what they are doing on the internet

and aware of the application used. The internet is what we make of it. Let's make it a safe and positive place for everyone.

Cyberterrorism is the use of digital technology to conduct terrorist activities, such as attacking critical infrastructure, spreading false information, or conducting espionage. Cyberterrorists may aim to cause fear, chaos, damage, or death among the public or specific groups. Cyberterrorism poses a serious threat to the security and stability of society.

Another form of cybercrime is cyberbullying, which is the use of internet platforms to harass, intimidate, or blackmail someone. Cyberbullies may use social media, instant messaging, or email to spread rumours, share embarrassing images or videos, or engage in online harassment. Cyberbullying can have serious psychological and emotional consequences for the victims, such as depression, anxiety, low self-esteem, or suicidal thoughts.
