A STUDY ON CYBER SECURITY ISSUES AFFECTING ONLINE BANKING AND TRANSACTIONS

N. VISHNUPRIYA,
POST GRADUATE STUDENT (M.COM)
JAIN DEEMED-TO-BE UNIVERSITY, BANGALORE
TANUSHA P
POST GRADUATE STUDENT (M.COM)
JAIN DEEMED-TO-BE UNIVERSITY, BANGALORE
DR. P. BHUJANGA RAO
PROFESSOR & FACILITATOR,
JAIN DEEMED-TO-BE UNIVERSITY, BANGALORE

ABSTRACT

The study is dedicated to a thorough exploration of the evolving cybersecurity challenges confronting online banking and transactions. In the digital age, as online financial services continue to become a cornerstone of our daily lives, it is paramount to understand, assess, and mitigate the risks posed by cyber threats. The study's objectives encompass a wide array of pertinent issues, from phishing and malware to identity theft and data breaches, while also delving into regulatory and compliance hurdles, mobile banking vulnerabilities, insider threats, and the implications of emerging technologies. By examining these challenges, the study seeks to provide valuable insights and practical recommendations for individuals, financial institutions, and regulatory bodies, ultimately aiming to fortify the security and trustworthiness of online banking and transactions in today's digital financial landscape.

Keywords: *Cybersecurity challenges, Online banking risks, Phishing and malware, Identity theft, Data breaches, Regulatory hurdles*

INTRODUCTION

In an era characterized by the pervasive use of digital technology, the banking and financial industry has undergone a significant transformation. Online banking and digital transactions have become integral components of our daily lives, offering convenience and accessibility to users. However, , this digital evolution has also given rise to a myriad of cybersecurity challenges and concerns that affect the security and trustworthiness of online banking and financial transactions.

The objective of this study is to examine the cybersecurity issues that impact online banking and transactions, shedding light on the risks and vulnerabilities that users, financial institutions, and regulators face in the digital realm. With the increasing reliance on technology for financial activities, it is imperative to understand and address these issues to ensure the safety and integrity of our financial systems.

Online banking and digital transactions have undoubtedly revolutionized the way we manage our finances. They offer numerous benefits, including 24/7 accessibility, faster and more convenient services, and reduced operational costs for financial institutions. However, this convenience comes with a price, as the digital realm is susceptible to a wide range of cybersecurity threats that can compromise the privacy and security of users' financial information.

This study aims to provide a comprehensive overview of the aforementioned cybersecurity issues, offering insights into current trends, potential solutions, and best practices to enhance the security of online banking and financial transactions in an increasingly digital world.

REVIEW OF LITERATURE

Ana Rita D. Rodrigues, Fernando Teixeria, Fernando A. F. Ferreria, Constantin Zopounidis (Jan 2022) The use of new technologies by traditional banking transactions is currently under intense demand from stakeholders. However, data security cannot be compromised because of the fundamental essence of this industry. A crucial component of the connections that exist between banking organisations and their customers is the level of confidence that users have in their bank branchers. The success, ability to draw in new business and ability to keep hold of current clientele are all strongly impacted by banks reputation. Because of these problems, judgements about how to approach the difficulties of integrating cyber – security, digital transformation, and AI into the banking industry are difficult to make.

Leandre Gomes, Abhinav Deshmukh, Nilesh Anute (2022) The majority of individuals now prefer to transact using E-banking, which has become a crucial component of the financial system. Customers benefit from internet banking, but they still need to exercise caution to protect their accounts from hackers and cyber-criminals because anything on internet is vulnerable to security risks. When compared to the ever-evolving cyber-dangers, the internet security protocols that most bank websites use to safe-guard their data are out of date. Due to these issues, it is simple for hackers and other outside parties to obtain private financial data. While there are a number of securities pre cautions to stop breaches, there are still flaws in these systems.

R. P. Manjula and Dr. R. Shnumughan (2016), In this case, the two fundamental rules governing real-time electronic surveillance in other criminal investigations also apply. One of those laws is search warrants, which allows authorities to enter the location where the cracker is thought to have evidence of the crime. The computer used to commit the crime, the software used to obtain unauthorised access, and other proof of the crime would all be considered examples of such evidence. The study's primary goal is to examine consumer perceptions about cybercrime and the cyberspace. In order to analyse the data, chi-square and percentage analysis were employed on a sample of 120 respondents. The conclusion is that in order to lower cybercrime in the future, more customer awareness campaigns should be held.

Wakil Ghori (2017) The public with digital banking accounts can access them from any location in the globe. The difficulties and security concerns pertaining to digital banking are discussed in this study. This essay discusses the difficulties and security concerns associated with online banking. This study also presents several fraud schemes, protection techniques, and cyberattack kinds that are employed by digital banks. This study examines internet banking security and safety concerns.

Xiang liu, Sayed Fayaz Ahmad, Muhammad Khalid anser, jingying ke, Muhammad irshad, Jabbar ul- haq, shujaat Abbas (2022) Vol 13. Cybersecurity concerns become more and more of a burden for businesses globally. The conceptual examination of malware, denial of service, social engineering, and attacks on personal data forms the basis of this research. We contend that applying contemporary technology to cybersecurity and e-commerce problems is an endless game of cat and mouse. Reliable technology is required to lower hazards, as is customer and employee training for technology use, as well as firm-wide policies and regulations.

Renata Marcinauskaite, Indre Pukanasyte, Jolita Sukyte (2019) This research study examines many aspects of the meaning and definition of unauthorised access to an information system (IS), considering international agreements, EU laws, and pertinent Lithuanian case law. The study addresses the components of unauthorised access to an IS while also resolving the wording and technology conundrum. Given the advancements in Lithuanian case law, there is a greater focus on the contentious violation of security measures as well as on its element.

Raheela Firdaus, Yang Xue, Li Gang, Muhammad Sibt e Ali (2022),This research is very significant for banks directly and for other people in society like bank customers who suffered from cybercrimes indirectly. Honest staff members could be rewarded and dishonesty should be punished so that no one tries to avail themselves of these kinds of opportunities. There should be strict supervision, and everyone should be held accountable for their responsibilities. People should use their skills in a positive way. At the last, banks need to implement Artificial Intelligence properly to secure transactions.

Dr. Erdal Ozkaya, Milad Aslaner (2019) The book starts out by giving you a general overview of cybersecurity and walking you through some of the most significant services and technology that are now vulnerable to online attacks. As you go through the chapters, you'll find flaws and vulnerabilities (including human risk factor), giving you an expert's perspective on the latest dangers. After that, you'll research methods for protecting infrastructure and data

Sarika R Lohana (2020) Cyberspace is susceptible to a wide range of events, whether deliberate or unintentional, manmade or natural, and both nation-states and non-state actors may use the data shared there for malicious ends. Governments, corporations, and individuals are all vulnerable to cyberattacks and threats. Being cautious with our data and keeping it out of the hands of fraudsters and scammers is the only way we can defend ourselves against such actions. Concerns about cyber security and digital banking are covered in this book in an enlightening and thorough manner.

Shadi A. Alijawarneh (2016) Customers and banks alike have benefited greatly from technological advancements in the banking industry; however, the use of e-banking raises vulnerability to system threats and attacks, making

effective security measures more important than ever. This book is ideal for professionals, practitioners, upper-level students, and technology developers interested in the latest advancements in e-banking security. It presents emerging techniques to secure these systems against potential threats and highlights theoretical foundations and real-world case studies.

Kannan Balasubramanian, K. Mala, M. Rajakan (2016) Many positive developments in the electronic world have resulted from technological advancements, particularly in the area of online commerce. The difficulties in securing online transactions and applications are covered in Cryptographic Solutions for Secure Online Banking and Commerce. A vital resource for financial planners, academics, researchers, advanced students, government officials, managers, and tech developers, this book highlights research on digital signatures, public key infrastructure, encryption algorithms, and digital certificates, among other e-commerce protocols.

Haitham M. Alzoubi, Taher M. Ghazal, Mohammad Kamrul Hasan, Asma Alketbi, Rukshanda Kamran, Nidal A. AL-Dmour, Shayla Islam (2022) The existence of many security concerns is one of the primary problems with this type of banking. The research uses a theoretical analysis method involving secondary information sources; it has also been able to bring forth some hypotheses about this topic, which it has also been able to support by using the statements and graphical charts provided by other authors in their previous works about this topic. The research topic is intriguing and can be used to do further research in the future. The majority of people are not even aware of or concerned about this matter.

Mrs. Kalpana nayar, Priyanka rathod (2021) Cyberspace refers to the virtual realm of the Internet, and cyber laws are the rules that regulate it. As a result of cyber laws' quasi-universal jurisdiction, all netizens, or internet citizens, are subject to them. Hacking, phishing, spamming, and other crimes where a computer is the target or is utilised as a tool to conduct an act (child pornography and hate crimes) are examples of cybercrimes. Computer crime is another name for cybercrime. Cybercriminals may access trade secrets from businesses, obtain personal information, or utilise the internet for malevolent or exploitative ends. This study focuses on the problems with cyber security that Indian banks are facing. Analysing the general public's awareness of cybercrimes is also beneficial.

Saqib Saeed, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri, Dina A. Alabbad (2023) This article on a literature review emphasises the significance of having a thorough understanding of cybersecurity risks when implementing digital transformation (DT) in order to avoid disruptions brought on by malevolent acts or unapproved access by intruders seeking to alter, destroy, or take advantage of users. At the end, we address potential future hazards related to the adoption of DT and offer suggestions on how businesses might reduce these risks by putting in place reliable cybersecurity safeguards. In order to help corporate organisations get ready to undertake digital transformation, the study suggests a framework for phased cybersecurity preparation.

Tong Xin, Ban xiaofang (2014),This paper discusses crucial questions about how to assess the security risks associated with online banking. Using this approach, we build the STRIDE threat model based on the examination of the important business data for the online banking system, and we build the threat tree based on the layer-by-layer decomposition of the security threat. As a result, it provides a thorough threat analysis of the online banking platform. This security threat analysis is crucial for identifying the threats that online banking is facing and for assessing the security of the online banking system.

Victoria Wang, Harrison Nnaji, and Jeyong Jung (2020), The results of this research report show that the Nigerian cybercrime sector has changed from low-tech cyber-enabled crimes to high-tech sophisticated breaches, with the top three most common breaches being hacking, viruses, worms, or Trojan infections, and electronic spam messages. Banking workers have had sufficient management in terms of support and training when it comes to cyber security procedures.

Hemraj Saini, Yerra Shankar Rao, T. C, Panda (2012) Online attacks might be processed unintentionally or with a purpose. Cybercrimes are defined as intentional attacks that cause significant disruptions to society, including economic disruption, psychological disorders, threats to national security, and more. Cybercrimes must be properly analysed in order to be restricted, and their effects on society at large must be understood. As a result, the present paper offers an explanation of cybercrimes and their effects on society, together with predictions for future developments in cybercrimes.

Nir Kshetri (2019) Regarding cybercrime activity, Africa has been one of the regions with the quickest growth rates. Not insignificant cyberattacks directed towards the rest of the world originate from the continent as well. Nonetheless, a lot of steps have been done to enhance cybersecurity across the continent and combat cyberthreats. Numerous nations on the continent have enacted laws to combat cyberthreats. Additionally, they have made enforcement actions more robust. Additionally, the private sector has made steps to improve cybersecurity.

OBJECTIVES OF THE RESEARCH

1. To assess the current state of cybersecurity in online banking and transactions.
2. To Examine the impact of cyber threats on online banking and financial transactions.
3. To analyse the effectiveness of current security practices and measures.

4. To evaluate the adequacy and efficacy of existing security measures in online banking
5. To Identify best practices and strategies for enhancing cybersecurity in online banking.

DATA COLLECTION PROCESS

The process of collecting data involves a methodological approach to obtaining information for research or analysis. The process initiates with the establishment of defined objectives and the identification of the required data sources, which may consist of surveys, observations, interviews, or pre-existing databases. Accuracy and relevance to the goals are ensured by choosing suitable techniques and creating customized instruments for data collecting.

Primary Data

Questionnaires are used to gather primary data for research on cybersecurity in online banking, both for users and institutions. These surveys provide preliminary data on user behaviours, security perceptions, and transaction-related issues. They provide important insights into the intricate details of cybersecurity and indicate potential weaknesses by disclosing experiences, opinions, and credentials of trust in online platforms.

Secondary Data

A study on cybersecurity in online banking can benefit immensely from secondary data, which includes databases, research reports, case studies of cyber events, and books and journals. These resources help with identifying weaknesses and landscape comprehension by providing statistical data, common threats, security measures, and insights into current breaches of security. They provide patterns, statistical data, and important insights into the nature of cybersecurity issues. This data's integration with primary sources enhances the study's scope as well as its depth.

SAMPLING TECHINQUES

Choosing an appropriate sample strategy is essential while researching cybersecurity in online banking. Ensuring representation across demographics or usage patterns is ensured by structured and random sampling. Quick, but potentially biased, convenience sampling is different from intended, and cluster sampling, which effectively target specific groups. These methods guarantee a sophisticated comprehension of cyber-security issues.

FREQUENCY TABLE

Particulars		Frequency	Percentage
Age	Below 30	25	75.8
	30 – 40	4	12.1
	40 – 50	3	9.09
	50 & Above	1	3
	Total	**33**	**100**
Gender	Male	14	42.4
	Female	19	57.6
	Total	**33**	**100.00**
Educational Level	Undergraduate	9	27.23
	Postgraduate	19	57.6
	PHD	1	3
	Others	4	12.1
	Total	**33**	**100.00**

Analysis: -

The provided data outlines the demographic distribution of a sample population based on age, gender, and education level. In terms of age, the majority of respondents are below 30 years old, constituting 75.8% of the sample, followed by those in the 30-40 age range (12.1%), 40-50 age range (9.09%), and individuals aged 50 and above (3%). The gender distribution shows a higher representation of females (57.6%) compared to males (42.4%). Regarding education levels, the majority have pursued postgraduate (PG) education, accounting for 57.6%, while 27.23% have completed undergraduate (UG) studies. Additionally, 3% of respondents hold a Ph.D., and 12.1% fall into the "others" category. This data provides insights into the composition of the surveyed group, revealing patterns in age, gender, and education distribution.

SI. No	Responses	Frequency	Percentage

DATA INTERPRETATION: -

1. **Respondents' opinions on using online banking services.**

1	Strongly Agree	21	63.7
2	Agree	8	24.24
3	Neutral	2	6.06
4	Disagree	2	6
Total		33	100.00

Strongly Agree (63.7%): The majority of participants strongly concur with the statement that they engage in online banking. Agree (24.24%): While not as much as those who strongly agree, a sizable portion do agree with the statement. Neutral (6.06%): A tiny portion of participants express neither agreement nor disagreement. Disagree (6%): A small percentage of participants don't agree with the statement.

In summary, the vast majority of participants engage in active online banking activities, indicating a favourable attitude towards this banking method. The comparatively low percentages of respondents who were neutral or disagreed indicate that online banking practices are generally accepted and used by the surveyed population.

2. **Respondents' opinions regarding potential cyber-security risks associated with internet banking are well-informed.**

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	11	34
2	Agree	17	51
3	Neutral	5	15
Total		33	100.00

The information displayed shows how respondents felt about the claim that "You are well informed about potential cyber-security threats related to online banking." 34% of participants strongly agreed with the statement, while 51% of participants agreed overall. 15% of respondents, on the other hand, expressed neutrality, and none of them expressed strong disagreement.

These results imply that respondents had an overall favourable opinion of their awareness of cybersecurity risks in relation to online banking. When there is neither disagreement nor strong disagreement, the sample appears to have a high degree of confidence or agreement about their perceived knowledge of the topic. This data can be useful in determining the group's general awareness and confidence regarding cybersecurity risks in the online banking industry.

3. **Respondents' opinions on being wary while disclosing private banking information online.**

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	19	57.6
2	Agree	10	30.04
3	Neutral	3	9
4	Disagree	1	3
Total		33	100.00

The provided data shows how respondents felt about the statement, "I am cautious about sharing personal banking information online." A substantial majority—57.6%—showed that they strongly agreed with the statement, which emphasises the need for extreme caution when disclosing personal banking information. Furthermore, 30.04% of respondents indicated agreement, indicating a strong general consensus regarding the significance of caution. Merely 3% disagreed with the statement, and only 9% of respondents were neutral. Remarkably, none of the respondents expressed strong disagreement.

These results highlight a general awareness and prudence among the respondents about sharing private banking information online, suggesting a generally responsible and watchful attitude towards protecting their financial information in the digital sphere.

4. The respondents' opinion of their awareness of the possible risks involved with utilising financial apps or services from third parties that connect to their online banking accounts.

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	16	49
2	Agree	11	33
3	Neutral	4	12
4	Disagree	2	6
Total		33	100.00

The provided data shows the opinions of those surveyed regarding the claim that "I am aware of the potential risks associated with using third-party financial apps or services that link to your online banking account." Notably, 49% of respondents strongly agree with this statement, indicating that they are well aware of the possible risks involved in integrating their online banking accounts with third-party financial services. Furthermore, 33% indicate agreement, highlighting the broad agreement regarding the significance of comprehending these risks. 12% of respondents are neutral, suggesting that there is a minority that does not have a strong opinion on the subject; 6% disagree, and 0% strongly disagree.

Overall, these results point to a general awareness among those surveyed of the possible dangers connected to third-party financial apps or services that are connected to online banking, highlighting a generally informed and cautious approach within the sampled group.

5. Based on respondents' opinions, financial institutions ought to give customers' privacy more weight than the gathering of data for security purposes.

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	16	48
2	Agree	12	37
3	Neutral	5	15
Total		33	100.00

48% of respondents strongly agree with this viewpoint, indicating a strong belief in the importance of protecting customer privacy over gathering a lot of data for security reasons. Furthermore, 37% of respondents indicate agreement, demonstrating a strong consensus regarding the significance of prioritising customer privacy. The remaining 15% are indifferent, suggesting that some respondents had no strong feelings about the issue. Remarkably, none of the respondents disagreed or strongly disagreed.

Overall, these results point to a widely held belief in the importance of protecting personal data while putting security measures in place among the surveyed group, supporting the prioritisation of customer privacy in financial institutions.

6.Respondents' opinions on using antivirus or extra security software in particular to protect my online banking activity.

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	11	33
2	Agree	11	33
3	Neutral	7	22
4	Disagree	3	9
5	Strongly Disagree	1	3
Total		33	100.00

33% of respondents strongly agree and agree that using extra security measures to protect their online banking is a good idea. This suggests that a sizeable percentage of the respondents are actively working to improve security. Moreover, 22% are neutral, indicating a sizable portion that has neither a strong preference for nor against the use of additional security software. All told, 12% disagree with the statement, with 9% disagreeing and 3% strongly disagreeing. This suggests that there may be a minority of people who do not think highly enough of extra security measures designed especially for online banking.

Overall, these results point to a varied but generally proactive attitude towards online banking security among the participants in the survey, with a significant number actively using antivirus or additional security software.

7.The opinions of respondents indicate that they think online banking platforms ought to offer their customers additional instructional materials regarding cyber-security.

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	13	39.5
2	Agree	13	39.5
3	Neutral	3	9
4	Disagree	4	12
Total		33	100.00

A sizable fraction, 39.5%, strongly agree and agree with this statement, suggesting that there is a general consensus among those polled regarding the need for online banking platforms to step up their efforts to offer cybersecurity education. Furthermore, 9% are indifferent, indicating a tiny percentage that has no strong feelings about the issue. However, 12% disagree, highlighting a minority opinion that might not give priority to the requirement for more cybersecurity education materials from online banking platforms. Interestingly, none of the respondents strongly

disagree. Overall, these results point to a strong desire among the surveyed population for better cyber-security education programmes, demonstrating a shared understanding of the value of providing users with the information they need to increase their awareness of online security.

8.According to respondents, banks disclose potential hazards and weaknesses in their online banking systems in a sufficiently open manner.

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	6	18
2	Agree	15	46
3	Neutral	9	27
4	Disagree	2	6
5	Strongly Disagree	1	3
Total		33	100.00

A significant proportion of those surveyed (46%) express agreement, of which 18% strongly agree and another 28% agree. This suggests that banks are transparent in disclosing potential risks and vulnerabilities in their online banking systems. Moreover, 27% are neutral, indicating a sizable portion of the population that has no strong feelings about banks' transparency in this area. With 6% disagreeing and 3% strongly disagreeing with the statement, 9% of respondents disagree. This suggests a minority opinion according to which banks do not disclose enough information about the dangers and weaknesses in their online banking systems.

The data indicates a wide range of opinions overall, with a sizable portion of respondents recognising transparency and a smaller portion voicing concerns about the amount of information banks provide regarding potential risks in their online banking systems.

9.Based on respondents, utilizing two-factor authentication for online banking is worthwhile since it adds an extra degree of security.

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	15	45.5
2	Agree	15	45.5
3	Neutral	2	6
4	Disagree	1	3
5	Strongly Disagree	-	-
Total		33	100.00

A sizable majority of respondents—91 percent—either strongly agree (45.5%) or agree (45.5%) with the statement, demonstrating the general consensus regarding the usefulness and effectiveness of two-factor authentication in boosting the security of online banking transactions. Furthermore, 6% of respondents are indifferent, indicating that there is a minority that has no strong opinions on the subject. Merely 3% disagree, highlighting a narrow perspective that might not adequately account for the ostensible security advantages of two-factor authentication.

Overall, these results show that there is broad agreement among those surveyed about the value and efficacy of adding two-factor authentication to online banking as an extra security measure.

10. Respondents' opinion regarding likelihood of implementing new security measures offered by banks to improve security of online banking.

SI. No	Responses	Frequency	Percentage
1	Strongly Agree	14	42
2	Agree	13	40
3	Neutral	3	9
4	Disagree	2	6
5	Strongly Disagree	1	3
Total		33	100.00

This statement was endorsed by 82% of participants, who either strongly agreed (42%) or agreed (40%) with it. This suggests that the surveyed individuals are very willing to accept and adopt new security measures that banks have put in place to improve the security of online banking. Furthermore, 9% are neutral, indicating a smaller percentage with no strong preference in either direction. In contrast, 9% disagree with the statement, with 6% disagreeing and 3% strongly disagreeing. This suggests a minority viewpoint that might be less likely to quickly accept newly implemented security measures by financial institutions. Overall, the data shows that the surveyed group was generally open to accepting new security initiatives that banks were introducing to increase the security of online banking transactions.

FINDINGS

A few findings may be obtained from a study on cyber security problems impacting online banking and transactions that uses respondents and a questionnaire. This is a visual representation of a possible findings listed below:

1. **Levels of Awareness:**
   - **Lack of Awareness:** A significant number of respondents may not be aware of common cyberthreats like phishing attempts or the significance of using strong passwords.
   - **Varied Understanding:** It's possible that respondents had different kinds of knowledge about online banking risk factors and security procedures.
2. **Usage Trends and Behaviours:**
   - **Frequent Usage:** A large number of respondents probably do frequent online banking transactions, suggesting a strong dependence on digital financial services.
   - **Device Preferences:** Individuals can indicate that they would prefer to use computers, cell phones, or tablets for banking transactions. Each of these options carries a certain level of security risk.
3. **Security Procedures & Measures:**
   - **Using MFA, or multi-factor authentication:** While some respondents said they would use multi-factor authentication (MFA) to protect their online banking accounts, others said they would only use passwords.
   - **Software Awareness:** Results might indicate a range of knowledge and use of firewalls, antivirus programmes, and other security technologies.
4. **Perception of Risks:**
   - **Data Privacy Concerns:** Most respondents may have expressed worries about the security and privacy of their financial information when making purchases online.

- **Threats Identified:** According to respondents, phishing, malware, and identity theft are the most common dangers.

5. **Education and Support Needs:**

- **Desire for Education:** A lot of respondents may have mentioned that more programmes pertaining to awareness and education about cyber security in online banking are needed.
- **Expectations from Financial Institutions:** It may be important to emphasise expectations about banks' and other financial institutions' accountability for guaranteeing the security of their customers.

The analysis of the respondents' questionnaire replies will yield important insights into the state of cyber security challenges that are now affecting online banking and transactions. This will make it possible to develop focused strategies to reduce risks and improve security measures.

SUGGESTIONS

Multi-factor authentication (MFA): additional security measure that goes beyond passwords. It might have to do with something you own (a mobile device or token), something you know (a password), or something you are (biometrics like fingerprints or facial recognition). Even with your password, it becomes considerably more difficult for attackers to obtain unauthorised access as a result of this.

Frequent Software Updates: Security patches are frequently included in the updates that operating systems, browsers, and banking apps issue on a regular basis. Updating your software and hardware on a regular basis keeps you safe against known flaws that hackers could take advantage among.

User Education: Banks should inform their clients clearly and continuously about typical cyberthreats, such as phishing emails and phoney websites. It's also a good idea to advise users to utilise password managers to safely store their strong, one-of-a-kind passwords for every online account.

Secure Networks: Using open Wi-Fi to conduct financial transactions puts your information at risk of being intercepted. Customer security is increased by recommending the use of virtual private networks, or VPNs (secure, password-protected networks) that encrypt data as it is transferred between devices and the internet.

Limited Access: Banks adhere to the least privilege principle, which states that employees are only given the minimal amount of access required to carry out their duties. As a result, there is less chance of insider threats causing harm and sensitive data exposure is restricted.

Constant Development and Adaptation: Cyberthreats are ever-changing. Banks must continue to be flexible and nimble, updating their security protocols on a regular basis, keeping up with new threats, and acting quickly to reduce hazards as they arise.

CONCLUSION

The reliability and security of online banking and transactions are continuously challenged by cybersecurity issues. There are many different kinds of risks in the world, ranging from cunning phishing attempts to sneaky malware and data breaches. Phishing attacks trick people into divulging personal information by using phoney emails or websites. Devices can become infected with malware, including ransomware, which can result in financial theft or hostage-taking of computers. The confidentiality of personal information is jeopardised by data breaches, making people more vulnerable to fraud and identity theft. These dangers not only cause large financial losses for people and businesses, but they also jeopardise the trust that underpins online banking systems.

The public collaboration becomes essential in the battle against security threats. Users, regulatory agencies, cybersecurity specialists, and financial institutions need to band together. Three essential elements of this cooperation include exchanging threat intelligence, putting regulatory frameworks into place, and encouraging innovation. Strict laws guarantee adherence to security requirements, fortifying the online transaction environment. It is essential for security technologies and processes to constantly innovate in order to keep up with the changing strategies used by cybercriminals. By working together, we can create a robust environment that discourages cyberattacks and increases trust in online banking services.

Essentially, an integrated strategy is necessary for preventing cybersecurity threats in online banking and transactions. It requires a strong technology foundation, user education, and stakeholder collaboration. In a world that is becoming more linked and delicate the integrity, confidentiality, and reliability of digital financial transactions can only be protected with a coordinated effort.

REFERENCES

1. Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today's online electronic banking systems. Computers & Security, 21(3), 253-265.
2. Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multistakeholder cognition-driven framework. Research in International Business and Finance, 60, 101616.
3. Gomes, L., Deshmukh, A., & Anute, N. (2022). Cyber Security and Internet Banking: Issues and Preventive Measures. Journal of Information Technology and Sciences (e-ISSN: 2581849X), 8(2), 31-42.
4. Umamaheswari, K., Dr. (2021, March 5). Impacts of Cyber Crime on Internet Banking. International Journal of Engineering Technology and Management Sciences. Available at SSRN: https://ssrn.com/abstract=3939579 or http://dx.doi.org/10.2139/ssrn.3939579
5. Ghori, W. (2017). Security Issues on Online Transaction of Digital Banking. International Journal of Scientific Research in Computer Science and Engineering, 5(1), 41-44.
6. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in Psychology, 13, 927398.
7. Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction fraud. Frontiers in Psychology, 13, 947234.
8. Ozkaya, E., & Aslaner, M. (2019). Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches. Packt Publishing Ltd.
9. Lohana, S., & Roy, D. (2021). Impact of demographic factors on consumer's usage of digital payments. FIIB Business Review, 23197145211049586.
10. Aljawarneh, S. A. (2016). [Book Title: Not provided]. Hershey, PA: IGI Global.
11. Balasubramanian, K. (Ed.). (2016). Cryptographic Solutions for Secure Online Banking and Commerce. IGI Global.
12. Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022, May). Cyber Security Threats on Digital Banking. In 2022 1st International Conference on AI in Cybersecurity (ICAIC) (pp. 1-4). IEEE.
13. Mandliya, I. P. (n.d.). A Study On Cyber Security Affecting Online Banking And Online Transaction (Doctoral dissertation, University of Mumbai).
14. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15), 6666.
15. Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415.
16. Dmitrović, V., Stojanović, D., & Jakovljević, N. (2021). Challenges for information and cyber security of banks in a pandemic environment and user attitudes. Covid-19, 129.
17. Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202-209.
18. Were, T. O. (2021). Implementation of UN Cyber Norms in the Promotion of International Security: a Case Study of Kenya (Doctoral dissertation, University of Nairobi).
19. Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea Preprints.
20. Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020, March). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (Vol. 270). Academic Conferences and Publishing Limited.