IJMCER

International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 6 ||Issue|| 3 ||Pages 579-606 ||2024||

Cyber security Challenges and Financial Technology Adoption Of Bank of The Philippine Islands In Cavite South Laguna Area

JOVELYN C. DOÑASALES
A Thesis Presented to the Faculty of Graduate School Continuing Professional Education
Pamantasan ng Cabuyao

ABSTRACT: This study explores the cybersecurity challenges and adoption of financial technology by the Bank of the Philippine Islands (BPI) in the Cavite South Laguna Area. Employing a quantitative methodology, data was gathered via a questionnaire checklist administered to bank clients. The investigation prioritized areas such as phishing attempts, credential theft, account takeover, This study delves into the cybersecurity challenges bank clients in San Pedro and Biñan branches deal with. It focuses on account takeover, credentials stealing, and phishing attempts. The research shows that these are issues that clients frequently face, as attackers use sophisticated techniques like social engineering and misleading features to take advantage of weaknesses. The frequency of credential theft presents a serious security risk, especially regarding bank account access, but less frequent instances of illegal account settings or personal information alterations are still cause for concern. Adopting stronger security measures is important due to the increased danger of data breaches linked to frequent illegal access.

This study also examines how financial technology is being widely used, with a focus on robo-advisor apps and digital payments. Banks prioritize customer safety through instructional initiatives, and high adoption rates are noted. Peer-to-peer transactions are mostly conducted online, which reflects changing customer preferences. By enhancing transaction efficiency and simplicity, robo-advisor apps are integrated into online banking, demonstrating the industry's dedication to technological innovation. This research investigates the relationship between cybersecurity challenges and financial technology adoption. Contrary to expectations, the study finds no significant correlation between the cybersecurity challenges faced by bank clients and the adoption of financial technology by the bank. In conclusion, it is important to have strong security measures to counter the growing cybersecurity risks that come with the widespread use of financial technology. It emphasizes how crucial it is for banks to defend their digital infrastructure and shield their customers from changing cyber threats by promoting and implementing robust security measures.

KEYWORDS: *cybersecurity challenges, financial technology adoption, security measures*

I. INTRODUCTION

The banking industry is a leader in providing consumers with opportunities to access products and services through advanced technology (Malar et al., 2021). Globally, both traditional financial institutions and individual consumers have been significantly impacted by the introduction of Internet banking. Mobile banking is vital because it is more convenient and facilitates payments faster than traditional banking methods. These days, people tend to utilize Internet banking more than traditional banking methods. As a result, a significant number of people, particularly customers, use electronic wallets as an alternative to conventional ways of payment. Financial technology (FinTech) integration has significantly transformed the industry in a modern international banking landscape. FinTech companies are at the forefront of offering innovative financial products and services, leveraging technologies such as big data, artificial intelligence, blockchain, and cybersecurity (Sohns & Wójcik, 2020). The management of cyber risk in IT-based banking systems has become a critical factor emphasized by managers, regulators, and international organizations due to its potential adverse effects on banks and financial institutions (Khan et al., 2021). Additionally, the development of information technology and the acceleration of digital transformation in the international arena have contributed to the formation of modern and different approaches in the financial system, including the operating part of banks (Mykhailiuk et al., 2021). The adoption of e-banking is considered an innovative distribution channel for financial services due to rapid advances in e-banking applications and intense competence (Sikdar et al., 2019). E-banking paves the way for promoting common business structures and the banking industry. Even though it has the potential to become a tool that banks may use to cope with tough routines, it also opens the way for the development of common business structures. Banking companies are making use of cutting-edge information technologies to service their customers efficiently all year long, around the clock, and in a manner that will contribute to increased corporate expansion. Furthermore, the advent of new technologies, products, and services encourages new needs and demands by customers (Hosseini et al., 2020). Everyone has jumped on board with the latest trend in consumer technology, which is known as the e-wallet. People stand to benefit much from utilizing it as a result of the extensive number of services that it offers. E-banking offers a wide variety of services for customers, which provide them with value and create a competitive advantage over competitors, such as account checking, bill payment, transferences, or mobile phone text message notifications (Mostafa, 2020). The revolutionary improvements in the technology used in electronic banking have made it possible to conduct transactions with banks in more practical ways, mainly through the use of the Internet banking medium. Studies that have been done in the past on banking services that are enabled by technology have shown that factors such as service quality, functional quality, perceived value, employee-customer interaction, perceived usability, and perceived risk all affect consumers' experiences (Mbama. Ezepue. Alboul. & Beer, 2018).

How employees respond to phishing attempts received through corporate email systems is a tangible illustration of an essential scenario in which employees continue to impact the businesses they work for. Phishing is a common way that hackers use to gain access to internal networks, collect sensitive information from employees, and carry out other destructive acts. Over ninety percent of malicious software is sent over email, with spear phishing attempts as the principal infection vector (Purplesec, 2021). Because of the serious potential for damage, companies have begun focusing on ways to reduce the risk posed to their employees by phishing attacks. "Simulated phishing campaigns" are a standard method companies use to evaluate the efficacy of their anti-phishing efforts. During these campaigns, employees are sent emails designed to resemble those delivered during genuine phishing attacks. It's not all bad news, despite the importance of analyzing the number of employees who fall victim to these phony attacks (Canham et al., 2021). Employees might have positive reactions to phishing assaults, reactions that alert organizational representatives to the potential hazard. Unfortunately, many of these good responses are frequently eclipsed by failures (successful mock attacks). This is the case even though they serve as a crucial warning signal or beacon to the organization, indicating that something may be wrong. At a time when cybersecurity continues to be a top priority for leadership but funding for the essential resources is unable to keep pace with the ever-evolving threat landscape, it would be in the best interest of businesses to also devote considerable focus on the positive spectrum of employees' cyber behavior.

This study additionally considers the effects on employment in the banking industry in response to the shifting face of modern banking. At BPI in the Cavite Southern Laguna, the integration of modern technology and cybersecurity measures has changed the nature of banking jobs and demanded the establishment of additional roles and abilities. This change emphasizes the necessity for a workforce that can handle the new cybersecurity issues as well as new financial technologies. The goal of the study is to determine how these shifts are affecting the sector's employment patterns, including the need for upskilling current workers, the need for new roles, and its wider impact on career paths and job security. Furthermore, Pamantasan ng Cabuyao has approved and monitored this research, guaranteeing that it complies with strict academic and ethical guidelines. This body's approval serves as more than just a formality; it's evidence of the significance and urgency of examining the effects of digital innovations in banking, particularly how they pertain to employment and cybersecurity. This approval highlights the study's importance in advancing knowledge about how banks, such as BPI, address these issues and reorganize their workforces. The study's conclusions should help shape strategies supporting workforce development and technology developments, ultimately benefiting the banking industry and its customers.

Theoretical Framework /Conceptual Framework : The following theories will serve as the foundation of the study. The Technological Innovation System (TIS) and Routine Activity Theory (RAT) provide an established framework for studying financial technology adoption and cybersecurity issues. TIS supplies a systemic view of financial technology adoption and diffusion, while RAT offers a criminological perspective on cyber threats and prevention. This dual-framework method allows a complete analysis of modern banking technology and security.The Technological Innovation System (TIS) is an analytical framework that explores the development and diffusion of new technologies as dynamic and systemic processes. It originated from the work of Carlsson and Stankiewicz in 1991, who introduced it as a systems approach to analyze the economics of technical change (Markard et al., 2015). This framework is particularly relevant for examining the emergence and growth of new technological fields and industries, such as those seen in modern banking strategies. The TIS framework can be applied to understand how innovations such as Artificial Intelligence, Biometric Data, Consortium Data, and

High-Tech Standardization evolve from novel ideas into integral components of the banking industry. The TIS framework views these innovations not as isolated events but as part of a complex network of agents, including financial institutions, technology developers, regulatory bodies, and customers. These agents interact under a specific institutional infrastructure that supports the generation, diffusion, and utilizationof these technologies.

Routine Activity Theory, introduced by Cohen and Felson in 1979, has been a crucial perspective in understanding crime, including cybercrime. The theory posits that for a crime to occur, three elements must be present: a motivated offender, a suitable target, and the absence of a capable guardian (Köhler et al., 2020). This framework is apt for analyzing various forms of cybercrime by assessing how cybercriminals (the motivated offenders) exploit vulnerabilities (the suitable targets) in the absence of effective cybersecurity measures (the capable guardianship).

II. RESEARCH PARADIGM

A concept is a set of comprehensive ideas taken from related fields of inquiry and used to assemble a succeeding presentation (Kombo and Tromp 2009, as quoted 2015). The paradigm for this study is illustrated below.

The study's visual model is represented in the diagram. It is intended to demonstrate the relationship between two sets of variables in this study that is to be hypothesized. The conditions or interventions that the study modifies or examines to determine their impact on the dependent variables are known as the independent variables. This illustrates the proactive steps the banking industry undertakes to remain innovative and secure from cyber risks. The outcomes that the study assesses to determine whether the independent factors influence the dependent variables. These represent the variety of risks and strategies used by cybercriminals to jeopardize the safety of banking activities. The arrow in the middle suggests the direction of the study's hypothesis. This investigation aims to close the knowledge gap about the connection between cybersecurity concerns and the uptake of financial technology solutions.

Thus, the figure illustrates a theoretical cause-and-effect relationship.

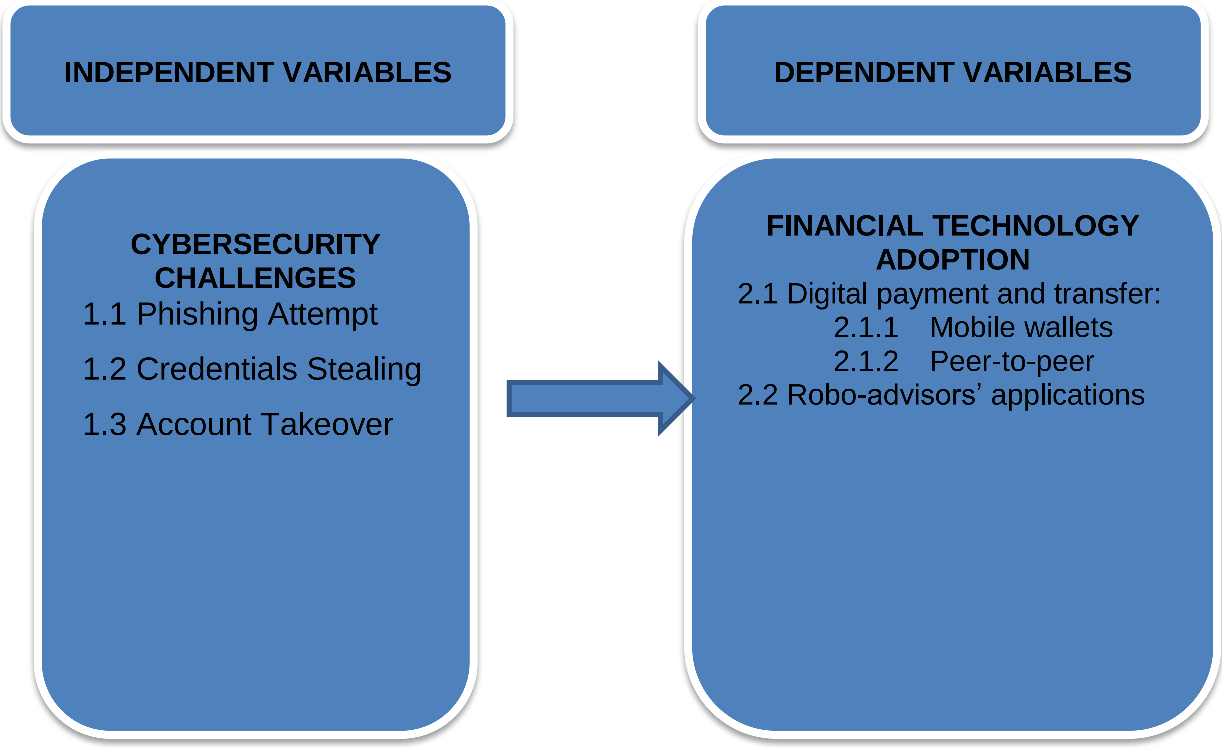


Figure 1. Research Paradigm of the Study

Research Questions

The purpose of this research study is to answer the following questions:

1. What is the level of cybersecurity challenges experienced by the bank clients in terms of:

✓ Phishing Attempt;
✓ Credentials Stealing; and
✓ Account Takeover?

2. What is the level of financial technology adoption on online banking in terms of:

- ✓ Digital payment and transfer:
- ✓ Mobile wallets
- ✓ Peer-to-peer
- ✓ Robo-advisors' applications?

3. Is there a significant relationship between the level of cybersecurity challenges experienced by bank clients and financial technology adoption in online banking?
4. Based on the study's findings, what client banking security measures may be proposed?

Hypothesis
The hypothesis to be tested for its significance:
Ho1: There is no significant relationship between the level of cybersecurity challenges experienced by bank clients and financial technology adoption in online banking.

Scope and Limitations : The study's scope and limitations provide openings for future research. This study has focused on improving mobile banking adoption among working professionals in Biñan and San Pedro Laguna, influencing people's eagerness to adopt a new system. This study aims to investigate the state of cybersecurity issues about the banking industry's embrace of financial technology, or FinTech. The focus of the topic is on examining the particular difficulties that financial institutions go into when implementing and integrating different FinTech solutions. Important topics like account takeover, credential theft, and phishing efforts will be covered in depth by the study. The study aims to offer a comprehensive understanding of the difficulties faced by financial institutions in guaranteeing the safe implementation of innovative financial technologies by concentrating on the cybersecurity element of FinTech adoption in banking. The results of this study will be useful in understanding the FinTech adoption in the banking industry and the larger cybersecurity landscape. This will help in the development of focused initiatives to improve financial institutions' security posture in the quickly evolving digital world.

Significance of the Study : It is of the utmost importance to increase digital literacy, and more especially knowledge about phishing, given the fact that phishing attempts are not going away any time soon. This article will emphasize how a person can distinguish phishing emails from legitimate ones and what tools they can use, including the output of this paper, which is a game about recognizing red flags in an e-mail or SMS that may indicate that it is a phishing attempt. In addition, this paper will discuss the resources that can be used.
The beneficiaries of this paper will be the following:

Clients. The cybersecurity precautions and awareness would improve their banking services and make their experience safer and more effective.

Employees. By applying the knowledge and insights this study provides, staff members may be better prepared to execute their jobs more effectively and pursue possibilities for professional growth in the areas of cybersecurity and contemporary banking technologies.

Other Banks. Utilizing the results to compare their cybersecurity defenses and plans, other financial institutions may work together to fight cyber threats and strengthen the industry as a who

Every Internet user. Everyone, including students, instructors, older citizens, and others, will benefit from being aware of the indicators of a phishing attempt, including:

Corporate. Companies should worry more about the possibility of their information being stolen by an employee unaware of phishing indications. This may lead to the attacker having access to the employee's account or gaining knowledge that another company can use to have an advantage over the other.
Future Researchers. Future researchers will benefit from this work because they will be able to continue this project or reference it as part of their thesis.

Definition of Terms
Credentials Stealing. This will involve analyzing how cybercriminals exploit weak passwords or security questions, which serve as suitable targets, and how the absence of multi-factor authentication reduces guardianship.

BPI. Bank of the Philippine Islands commonly known as BPI; PSE: BPI) is a universal bank in the Philippines. It is the first bank in both the Philippines and Southeast Asia. It is the fourth largest bank in terms of assets, the second largest bank in terms of market capitalization, and one of the most profitable banks in the Philippines.

Credentials Stealing. This will involve analyzing how cybercriminals exploit weak passwords or security questions, which serve as suitable targets, and how the absence of multi-factor authentication reduces guardianship.

Cybersecurity. The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Cybersecurity Challenges. Cybersecurity challenges refer to the various threats and vulnerabilities in modern banking such as; phishing attempts, credentials stealing, account takeover, money laundering, and accounting fraud.

Fraud. Refers to the intentional perversion of truth to induce another to part with something of value or to surrender a legal right.

Modern Banking. The bank is one of the most important financial institutions. It provides several services to consumers around the world.

Modern Banking Strategies. Modern banking strategies refer to the innovative approaches and techniques that banks and financial institutions employ to stay competitive, improve customer experience, and increase profitability such as; artificial intelligence, biometric data, consortium data, and high-tech standardization in financial settings.

Phishing. The fraudulent practice of sending emails or other messages purporting to be from reputable companies induces individuals to reveal personal information, such as passwords and credit card numbers.

Phishing Attempt. It can help understand how phishing scammers identify vulnerable targets, such as employees without proper cybersecurity training, and exploit these targets where digital "guardians" like anti-phishing tools or protocols are lacking.

III. REVIEW OF RELATED LITERATURE AND STUDIES

This study section presents a literature review on cybersecurity challenges and financial technology adoption. Since this will highlight the importance of the investigation, it will serve as a cornerstone for the research. This part aims to highlight or identify the potential that has been overlooked in earlier studies and to provide an overview of the studies that have already been made in prior years.

Conceptual Literature : Mobile banking in the Philippines has not taken off despite the country having 148.71 mobile-cellular telephone subscribers per 100 people (ITU, 2020) and banks expanding and innovating via online banking. Access to financial services is limited in the Philippines, an archipelago of more than 7,000 islands, where most transactions take place in cash or through unbanked, face-to-face interactions. Small business owners, farmers, and fishermen may not perceive the benefit, and many people lack the resources to use the Internet. This group was hesitant to try out new financial advancements for fear of losing everything.

According to the study by Sonowal (2022), the widespread problem of phishing is the fraudulent act of posing as a reliable source in online contacts to get private information such as passwords, usernames, and social security numbers. Phishing assaults have increased significantly in regularity in recent years, costing both individuals and organizations a great deal of money. Citing Verizon's 2020 Data Breach Investigations Report (DBIR), it states that 22% of all breaches in 2019 involved phishing, with 65% of US firms falling victim to successful phishing assaults. His book covers a wide range of phishing attack types, including DNS-based, search engine, content injection, and deceptive phishing. It also covers the many communication channels—voice, SMS, email, blogs, and wifi—that are regularly used by attackers. Readers will also learn more about phishing kits and how security professionals utilize them to raise user awareness. The book presents thorough solutions, including educational, legal, and technical measures, to protect people and organizations from phishing threats. It also gives a knowledge of common strategies used by attackers to obtain information. The core target comprises those who interact with banks, online retailers, payment systems, government agencies, social networks, blogs, IT firms, and telecommunications companies.

Furthermore, Riadi et. al. (2023), discuss that through mobile security lab testing, the Anubis Trojan is evaluated to uncover its wide range of capabilities. These include the development of applications for SMS sending, keylogging, SMS spam, executing commands for the Remote Access Trojan (RAT), retrieving call history, turning off Play Protect, and sending information to attackers via a Command and Control (C2) Server. Users are forced to enable an access service that secretly records all user activity while running in the background by the Anubis Trojan, which is the source of these malicious activities. It is advised to only download apps from reliable sources, update the software frequently, and enable security settings to protect Android devices against Anubis assaults. Further strengthening defenses against Trojans like Anubis is possible by utilizing Google Play Protect.

Meanwhile, Castell (2020) discusses the Zeus malware, discovered in 2007, has changed its source code, presenting a challenge for antivirus software to detect. Mainly distributed through phishing and man-in-the-browser (MITB) attacks, Zeus infects users' browsers, functioning independently or altering user actions in real-time. It lies dormant until users visit specific sites like online banking, where it intercepts and modifies transaction details after authentication. The leak of its source code in 2011 facilitated its widespread use.
Najib, M., & Fahma, F. (2020) focus on the Technology Acceptance Model (TAM). This study aims to better understand the intention of Small and Medium Enterprises (SMEs) to implement digital payment systems, specifically in the Indonesian restaurant industry. Taking into account the distinct commercial and technology environment in Indonesia, the study established the trust variable. The suggested model seeks to offer SMEs a thorough grasp of the adoption of digital payments while also providing insights into the behavior of technology adoption in this particular setting. The study found that the main factors impacting SMEs' attitudes and intentions to utilize digital payment systems were perceived usefulness, perceived ease of usage, and trust.

Research Literature : Cybersecurity in modern banking faces numerous challenges, including the need to intertwine safety and security during risk assessment This is reflected in the significant investments made by governments and financial institutions to improve cybersecurity prevention and protection (Morgan et al., 2020). The technical development and exploration of deep learning (DL) methods in cybersecurity present challenges. DL techniques are not a panacea but rather a tool that requires correct and trustworthy features to be effective (Meister et al., 2020). Additionally, the use of artificial intelligence (AI) in cybersecurity is crucial, especially in the context of healthcare systems, where AI can help address, vulnerabilities compromising data confidentiality, integrity, and availability, particularly in the era of Covid-19 (Majumder & Veilleux, 2022). Furthermore, the fintech industry, which is closely related to modern banking, presents both challenges and opportunities. While it offers potential, companies in this space must navigate complex regulations, address cybersecurity risks, build consumer trust, and compete with traditional financial institutions (Ameen & Afşar, 2023). Moreover, the utilization of fintech applications in the banking and finance systems faces challenges, such as promoting their development and addressing cybersecurity concerns (Akdeniz, 2022).

Customers of electronic banking need to consider both the benefits and the drawbacks of using the service, although it is convenient and easy to use. According to Alknowiter (2022), every individual must make significant financial decisions due to the risks that bank customers are believed to represent regarding trust, privacy, and other aspects. E-banking is a distribution and communication channel that allows customers to interact with a bank to conduct economic and efficient transactions, mainly through electronic tools, e.g., tablets or smartphones (Singh and Srivastava, 2020). Basedit et al. (2020) conducted a thorough analysis of phishing attack detection methods enhanced by artificial intelligence. This study examines many Artificial Intelligence (AI) methods for phishing attack detection, such as Machine Learning, Deep Learning, Hybrid Learning, and scenario-based methods. This analysis provides insightful information on the developments in technology to thwart phishing efforts. Additionally, the research examines individual variations linked to behavior in a realistic phishing simulation (Beu et al., 2022). According to the report, dissatisfied and younger workers are especially susceptible to phishing tactics, underscoring the significance of focused cybersecurity training in reducing these risks. Furthermore, reexamines prior studies on phishing from a security standpoint, emphasizing the particular difficulties in active attacker situations, real-time detection, dataset quality, and base rate fallacy (Das et al., 2020). This reexamination emphasizes how customized security solutions are required to deal with the changing landscape of phishing assaults.Furthermore, the research highlights the significance of contextualization in people's susceptibility to phishing attempts, suggesting that messages customized for certain situations might take advantage of psychological weaknesses, making people more vulnerable to these kinds of assaults (Hassandoust et al., 2022In the digital age, cybersecurity issues in contemporary banking, especially about credentials theft, have grown to be of utmost importance. A serious risk to banking security is phishing, a dishonest tactic used to get private data including bank account information and login passwords (Rahim ZA&

Basheer, 2021). According to Tharani and Arachchilage (2020), fraudsters have also been known to utilize machine learning methods to imitate uniform resource locators to leverage phishing assaults on their targets. Additionally, it has been noted that one way to obtain unauthorized access to private financial data is by using SQL injection attacks to steal login credentials (Chaki et al., 2019). Holovkin et al. (2021) have detailed the contemporary difficulties of cybersecurity in the fight ag

ainst corruption, highlighting the need to ensure cybersecurity in the financial industry. According to Kuzmenko et al. (2020), the utilization of contemporary technology for electronic payments, mobile banking, and payment processing has brought up new hazards, such as fraudulent transactions and account takeover. Moreover, the banking sector needs strong cybersecurity measures because of the development of cyberattacks and industrial problems (Vishwanath, 2023). The banking industry must take into account several cybersecurity-related issues, such as the enactment of cybersecurity legislation and the evaluation of banking clients' understanding of cybersecurity (Bokhari, 2022). Furthermore, an approach to improve security and lessen account takeover assaults is the implementation of risk-based authentication systems (Wiefling et al., 2021)There is a correlation between concerns over privacy and security and monetary losses (Cheng et al., 2022). Both of these issues have been identified as significant trust concerns (Wang and Shan, 2019) and barriers to the widespread use of mobile commerce (Gao and Bai, 2019). To bank customers, privacy means that their private data is safe from prying eyes and cannot be intercepted or stolen (Cheung and Lee, 2021; Mukherjee and Nath, 2021; Lee, 2022; Lee and Turban, 2021; Littler and Melanthiou, 2022; McKnight et al., 2021). It abides by laws and codes of conduct, such as those that forbid private companies and governments from using or misusing an individual's data (Agranoff, 1991; Casaló et al., 2022).

To help governments and businesses gauge the level of cyber maturity in their respective nations, Feakin et al. (2019) created a "cyber engagement scale" comprised of indicators in the areas of governance, crime, the military, business, and society. The presence, successful implementation, and functioning of cyber-related structures are indicators of maturity, according to Feakin et al. (2019). They discovered that the Philippines' government remains unresponsive, has inadequate enforcement, is unaware of cyber military challenges, and fails to engage the private sector and industry in developing the digital economy through smart public policy.
Due to these vulnerabilities, the country has been subject to sophisticated cyberattacks, including e-mails laden with viruses and malware, attacks on websites, and the laundering of illicit funds, among other crimes. "87 percent of Filipino internet users were identified as victims of crimes and malicious activities committed online" (Avendano, 2019), according to a report by the Department of Justice (DOJ). From 2020 to 2019 (Felipe, 2019), internet fraud was the most often reported cybercrime to the Philippine National Police. The "I Love You" virus in 2021, government website hacking in 2021, the "Heartbleed Bug" in 2019, the hacking of the Commission on Election (Comelec) website in 2016, and the Bangladesh Central Bank cyber heist in 2016 are all examples of significant events of cybercrime in the Philippines.

In addressing these challenges, innovative strategies that efficiently integrate modern technologies, such as AI and advanced electronic systems, are required (Stawicki et al., 2022). This is crucial for modern banking to navigate the complexities of cybersecurity and ensure the confidentiality, integrity, and availability of financial information. Additionally, the interconnected nature of safety and security in risk assessment emphasizes the need for robust cybersecurity requirements that can be traced back to their source, such as a barrier (Meland et al., 2019).The adoption of financial technology in online banking has been a subject of interest. Several foreign literature pieces have contributed to understanding the factors influencing the adoption of financial technology in online banking. Górska et al. (2022) highlighted attitudes towards online social interactions and technology during the COVID-19 pandemic. The study identified psychological resilience, optimism, innovativeness, self-efficacy, habit, social influence, risk-taking, and individuals' perception of their security online as traits and factors moderating human-technology engagement and adoption. These findings are crucial in understanding the psychological aspects influencing the adoption of financial technology in online bankingNugrahini & Alfian (2021) focused on the impact of the continuance adoption of mobile payments. Their conceptual framework emphasizes the role of technologies such as mobile banking in enabling users to access information about their balances and transactions, thereby strengthening user adoption intentions. This framework contributes to understanding the continued adoption of mobile payments, which is highly relevant to the context of online banking. Ameen & Afşar (2023) address the impact of fintech on money laundering, noting the speed and difficulty of detecting such operations in modern banking technology and highlighting the role of the Central Bank of Iraq in granting licenses to fintech companies. This reference is relevant as it discusses the impact of fintech on modern banking technology, particularly in the context of money laundering and regulatory aspects, which are significant considerations in the adoption of financial technology in banking.On the other hand, the development of financial technology is currently growing, which can be seen in online shopping services and access to fast and efficient banking services. This reference is relevant as it highlights the growth of financial technology, particularly in providing fast and efficient banking services, which is pertinent to the adoption of financial technology in modern banking Susanti et al. (2023).

Meanwhile, in the context of local banking, the role of local banks in providing access to capital and financial services to the community is significant. Local banks tend to rely more on soft information, which can play a crucial role in lending decisions, especially in regions where soft information could be more influential (Fairlie et al., 2022). The study of small business lending and regulation for small banks also emphasizes the positive effects of regulatory capital relief for the local economy (Srivastav & Vallascas, 2022). Moreover, networking, especially connections with government officials, can substitute local institutions by addressing weaknesses in legal enforcement, corruption, bureaucratic compliance, and non-transparent governance systems, thereby impacting small business investment (Nguyen, 2021).An article by Hamsin et al. (2022) aims to investigate and thoroughly assess the consistency of Islamic financial institutions in adopting Sharia principles. This is relevant as it explores the application of Sharia principles in financial institutions during the COVID-19 pandemic, providing insights into the dynamics of financial practices during challenging times. The adoption of digital payment transfer technologies has been the subject of extensive research in recent years (Pal & Ansari, 2020). highlighted the significance of mobile payments in facilitating convenient online transfer of funds, particularly in the context of the COVID-19 crisis relief fund collection in India. This underscores the relevance of digital payment mechanisms in addressing real-world challenges.

Additionally, Agrawal & Jain (2019) emphasized the importance of understanding people's behavior toward the adoption and use of banking services, particularly in the context of digital financial inclusion in India. Their focus on financial inclusion aligns with the broader goal of promoting the adoption of digital payment transfer technologies to enhance financial accessibilityMeanwhile, Pal & Ansari (2020) contributed to the understanding of mobile payments and online promotions in the context of crisis relief fund collection, shedding light on the potential of online promotions paired with mobile payments to enhance security and transparency. This provides valuable insights into the practical applications of mobile wallets in crises. Furthermore, Ankita & Trivedi (2023) discussed the potential impact of blockchain and distributed ledger technology on future banking, emphasizing the role of these technologies in increasing transparency and reducing costs, which could have implications for mobile wallet transactions. This literature collectively underscores the multifaceted nature of digital payment transfer adoption, encompassing technological, behavioral, and societal dimensions, particularly in the context of mobile wallet usage.

Meanwhile, (Chauhan et al., 2019), the study highlights the positive impact of perceived usefulness, ease of use, attitude, innovativeness, and perceived risk on consumers' intention to adopt Internet banking. This suggests that factors such as perceived usefulness and ease of use play a crucial role in influencing consumer behavior in the context of person-to-person financial technology adoption in online banking.Furthermore, (the Salem et al., 2019) study's findings indicate that technology adoption propensity is a significant factor influencing customers' usage of online banking services. The empirical evidence presented in the study emphasizes the importance of this factor in the context of Palestinian customers' adoption of online banking. This aligns with the task as it highlights the relevance of technology adoption in person-to-person online banking usage, providing valuable insights for understanding the factors influencing adoption in this specific domain.The literature on financial technology adoption, specifically focusing on digital payment transfer using robo-advisor applications, is crucial for understanding the evolving landscape of financial services. Among the provided references, Szabó et al. (2021) contributed to developing robo-advisors through design thinking-based ontology, which can provide valuable insights into the technological advancements in digital payment transfer.

Additionally, Chen & Dastane (2022) discussed advanced technological factors affecting digital banking usage intention, including artificial intelligence-based robo-advisors, which directly relate to the adoption of robo-advisor applications in the financial sector. These studies offer valuable perspectives on the integration of robo-advisor applications in digital payment transfer, highlighting the technological advancements and user intentions in adopting such innovative financial tools.(Dahab & Bouqlila, 2021) conducted a case study on E-payment adoption during the pandemic, enriching the existing literature on E-payment adoption models, particularly in the Moroccan market. The study provides valuable insights into the factors influencing E-payment adoption, shedding light on the impact of the pandemic on the adoption of online financial servicesIn contrast, Etambakonga (2021) discussed the rise of virtual reality in online courses and the ethical issues and policy recommendations associated with it. Although the focus is on virtual reality in online courses, the ethical concerns and policy recommendations may provide insights into the ethical considerations in the adoption of financial technology in online banking, especially as online banking increasingly incorporates virtual and augmented reality features.

The technological readiness (TR) paradigm (Parasuraman & Grewal, 2021) describes how users adapt to and make use of emerging technologies. As a measure of consumers' openness to new technologies, SST adoption can be influenced by TR (Liljander et al., 2022; Tsikriktsis, 2021). To better describe customers' intent to utilize electronic services, C. H. Lin et al. (2022) developed the TRAM model by integrating the TAM and TR components into a single model.In another study, Nguyen et al investigated Fintech applications' development in the Vietnamese banking industry alongside identifying challenges to promote Fintech applications in the banking and finance systems in Vietnam. This reference is relevant as it discusses the development and challenges of promoting fintech applications in the banking and finance systems, providing insights into the adoption of financial technology in the banking sector. The impact of a pandemic on financial institutions and financial markets Ozili (2022). This addresses the impact of a pandemic on financial institutions, which is crucial in understanding the challenges and dynamics of modern banking, especially in the context of adopting financial technology.

Research on the use of financial technology (FinTech) in the banking industry is becoming increasingly important, especially when it comes to digital banking. Many studies have looked at the relationship between mobile banking and bank performance the impact of digital financial inclusion on banking stability (Galazova & Магомаева, 2019), and the strategic adoption of digital banking to boost competitiveness and maximize benefits for shareholders.Furthermore, the research emphasizes how IT investments affect how clients become digital in the digital age and how traditional banking operations change as a result (Carbo-Valverde et al., 2020;). In addition, a great deal of research has been done on the elements influencing the uptake of digital bank services, including trust, security, financial literacy, and brand image. In (2022, Sumaylo et al.). Talk about how digital finance affects bank stability in the Philippines, emphasizing the framework the government has put in place to innovate and enhance payment systems. This will help you grasp the background of FinTech adoption in the nation. Burguillos & Cassimon (2021) investigate the variables influencing the expansion of financial inclusion throughout the Philippine territories. It is pertinent because it offers insight into the factors that influence financial inclusion, which is essential when discussing the use of financial technology in digital banking.

Awareness of the state of digital access and technology adoption in the Philippines requires an awareness of the focus of this article, which is on mobile technology adoption Roberts and Hernandez (2019). Sahay et al., (2021) the effects of financial technology adoption on the Philippine banking industry require an awareness of the role that digital financial services play in promoting financial inclusion in emerging markets and developing countries.Discusses how digital government may create new financial possibilities to boost economic growth and make governance more effective and less corrupt (Mobo, 2022). This demonstrates the wider effects of digitalization on financial development and governance and suggests that digital government programs might help promote the use of financial technology in the Philippines.Cui's (2022) study sheds light on the correlation between FinTech adoption and regional financial inclusion in China, emphasizing the disparities across areas that utilize FinTech to promote financial inclusion. This study is pertinent because it addresses how FinTech adoption affects bank risks and financial inclusion, which is a topic that is closely related to the challenge of comprehending FinTech adoption in the banking industry.In their 2023 study, Chouhan et al. investigate how FinTech is affecting India's traditional banking sector, paying special attention to the value propositions that encourage the use of banking products or FinTech. Because it examines the elements that influence FinTech acceptance and how it affects the banking industry, this study is relevant to the problem of understanding FinTech adoption in banking.

The adoption of FinTech services by banks and its possible influence on bank efficiency are the main topics of Maryunita & Nugroho's (2022) investigation on the relationship between FinTech innovation and bank efficiency in Indonesia. This study is relevant because it addresses the problem of comprehending FinTech adoption in the banking industry by offering insights regarding the technology's adoption from a bank-focused perspective.Zhong-Qing together with others. Relevant to the objective, Zhong-qing et al. (2019) investigate bank consumers' intentions to use FinTech services, offering insights into the variables driving FinTech service acceptance in the banking industry.Nowroozi et al. (2023) discuss the assessment and security of cryptocurrency wallets, emphasizing the growing demand for their usage due to speed, security, and the ability to conduct transactions between two users without the need for a third party. While the reference focuses on cryptocurrency wallets, it provides valuable insights into the factors driving the adoption of digital payment and transfer technologies, such as mobile wallets and peer-to-peer transactions, within the online banking domain.

Awwad (2023) investigates the uptake of FinTech in Palestine, stressing the dangers and obstacles of doing so as well as the inclination toward conventional banking practices. This study is significant because it sheds light on the difficulties of FinTech adoption in a particular banking environment. Rahman et al. (2020) relate the technological acceptance model with perceived security and trust in adopting mobile banking for financial services as they examine the intention to embrace mobile banking from a security viewpoint in Bangladesh. Because it focuses on the adoption of FinTech-related services in the banking industry, this study is pertinent.

In keeping with the challenge of comprehending the adoption of FinTech in the banking sector, Pierri & Timmer's (2021) study on the significance of technology in banking during a crisis is pertinent since it offers insights into the implications of information technology in banking for financial stability.Additionally, using a variety of technological adoption models and behavioral research, George & Sunny (2020) theoretically investigated aspects impacting behavioral intention and actual usage of mobile wallets, offering a thorough knowledge of the adoption process. Lin et al. (2022) discuss default risk prediction and feature extraction using a penalized deep neural network in the context of online peer-to-peer lending platforms. Specifically, it highlights the direct lending process between individuals through online platforms, which is relevant to the peer-to-peer transfer aspect of financial technology adoption in online banking. Furthermore, Lacap (2022) investigated the adoption of mobile wallets in the Philippines using a Partial Least Squares Path Modelling technique, offering insights into the usability and mediation elements of adoption.Furthermore, as evidence of the influence of outside forces on adoption, Garg & Goyal (2020) highlighted the rise in awareness of mobile wallet usage in India as a result of government initiatives like demonetization, which coerced people into using mobile wallets.

Eren (2023) explores the antecedents of robo-advisor use intention in private pension investments, shedding light on the factors influencing individuals' intention to use robo-advisors in an emerging market country. The study's focus on trust and financial risk tolerance aligns with the task's interest in robo-advisors' applications within the context of financial technology adoption in online banking. Additionally, the reference highlights the relevance of trust in shaping individuals' attitudes towards financial risk, which is crucial in understanding the adoption of digital payment and transfer technologies, such as mobile wallets and peer-to-peer transactions, within the online banking domain.

Mew & Millan (2021) also emphasized the main motivators and barriers to consumers' intention to use financial mobile apps, connecting Social Influence (SI) to the desire to use mobile credit cards, mobile payments, and mobile banking.Similarly, Gbongli et al. (2019) emphasized the usefulness of well-established models in a variety of situations by extending the Technology acceptability Model to forecast mobile-based money acceptability and sustainability in poor nations.Chou et al. (2023) focus on the complementary effects of bank intangible value binding in customer robo-advisory adoption. This provides valuable insights into the adoption of robo-advisors' applications within the context of online banking. The emphasis on the importance of bank intangible value binding in customers' robo-advisory adoption aligns with the broader theme of financial technology adoption in online banking, particularly in the context of robot advisor applications.The process of adopting mobile banking is complex and impacted by several variables, such as perceived utility, perceived usability, risk, trust, and social influence (Leon, 2019). underlined the need to expand on current models and add to the body of knowledge on factors influencing the use of mobile banking in the Philippines. The research also stressed the importance of ease, security, and trust in shaping adoption behavior. In highlighting the ease that mobile wallets provide, Enkono & Suresh (2020) for example, noted that m-banking enables users to transfer money from their bank accounts to other users' electronic wallet accounts.

In addition, systematic mapping research (Alexandri et al., 2023) found the influence of FinTech on investment decision-making in ASEAN banking. This is an important consideration. Peer-to-peer lending, blockchain technology, mobile banking, and advising platforms are the four major FinTech technologies that influence investment decision-making in ASEAN banking, according to this study, which reviewed 128 pertinent papers. Measuring the potential uptake of FinTech in the Philippines requires an understanding of these technologies' effects.

Synthesis : The adoption of mobile banking has been sluggish in the Philippines, despite a high mobile phone subscriber rate. This can be attributed to issues such as restricted access to financial services, dependence on cash transactions, and apprehensions over novel financial technologies. The hesitation can be attributed, in part, to the dread of phishing attempts, as Sonowal (2022) points out. Phishing has become a common problem in recent times. Zeus malware and the Anubis Trojan present additional risks, highlighting the necessity of effective cybersecurity defenses. The study conducted in Indonesia by Najib and Fahma (2020) highlights the significance of trust in SMEs' adoption of digital payment systems and identifies variables affecting attitudes toward technology.Protecting against cybersecurity threats—most notably, credentials theft—is critical in today's digital banking environment. Phishing is a serious risk since it uses deception to obtain private information (Rahim ZA& Basheer, 2021). According to Riadi et al. (2023), users should take precautionary steps including app vetting and software updates in light of Anubis's range of malicious capabilities, which include SMS spamming and remote access control. Castell (2020) draws attention to Zeus's versatility and how it's used in phishing scams directed at online banks. Further observations from Rahim ZA & Basheer (2021), Tharani and Arachchilage (2020), and Chaki et al. (2019) highlight the growing threats that SQL injection and phishing assaults represent to the banking industry. To fight corruption, particularly in financial institutions, Holovkin et al. (2021) emphasize the necessity of improved cybersecurity measures.

Ameen and Afşar (2023) shed attention on the difficulties in identifying money laundering in the context of the swift progress in financial technology (fintech) and underscore the regulatory function of organizations such as the Central Bank of Iraq. Susanti et al. (2023) highlight fintech's impressive rise, especially in terms of improving banking efficiency and online buying services, which is a sign of its growing incorporation into contemporary financial practices. In-depth analyses of local banks' critical roles are provided by Fairlie et al. (2022) and Srivastav & Vallascas (2022), who highlight the banks' contributions to capital availability and the benefits of regulatory relief for small banks and local economies—particularly in the area of small business lending.Morgan et al. (2020) explore the broad cybersecurity concerns in modern banking and emphasize the importance of deep learning and artificial intelligence integration, as well as good risk assessment. The fintech sector, which is intimately associated with the banking business, offers a range of opportunities and problems. These include the need to navigate intricate regulations, mitigate cybersecurity threats, and cultivate consumer trust (Ameen & Afşar, 2023). Research on AI-based techniques for phishing attack detection, as done by Basedit et al. (2020), highlights how cyber threats are constantly changing and how important customized security solutions are.

The use of financial technology in banking is a worldwide phenomenon, with research covering a range of nations and areas. Sumaylo et al. (2022) provide evidence from research conducted in the Philippines showing the government's framework is critical to innovation and the improvement of payment systems. According to Ozili (2022), the pandemic's effects on financial institutions shed light on the dynamics and difficulties of contemporary banking, particularly the adoption of financial technology. The literature explores user intentions, security issues, and the effects of government actions concerning the deployment of financial technology in banking. Research from a range of nations, including India (Gbongli et al., 2021) and China (Zhong-qing et al., 2021), adds to our understanding of the global trends in FinTech adoption. Studies such as Leon (2020) and Enkono & Suresh (2020) illustrate the complexity of the adoption process wherein perceived usefulness, usability, risk, trust, and social influence all play a role.

A comprehensive knowledge of this dynamic landscape is made possible by the global nature of cybersecurity risks, the significance of confidence in the adoption of new technologies, and the diverse effects of FinTech on the banking systems of other nations. To tackle these obstacles, cooperative endeavors, inventive tactics, and a profound comprehension of the constantly changing technological and regulatory landscapes inside the financial industry are needed.Eren (2023) explores the elements that precede the intention to use robo-advisors, highlighting the importance of trust and financial risk tolerance in influencing people's perceptions of the use of these emerging market robo-advisors. Mew & Millan (2021) and Chou et al. (2023) make additional contributions to this discussion by analyzing the factors that encourage and hinder users of robo-advisors and financial mobile apps, respectively. They emphasize the significance of social influence and intangible value binding. By highlighting the suitability of existing models in predicting the acceptability and sustainability of mobile-based money in low-income nations, Gbongli et al. (2019) expand on this conversation.

Research Gap : The examination of the literature delves deeply into the prospects and problems surrounding mobile banking, cybersecurity, and the adoption of financial technology in the Philippines. There are study gaps despite the abundance of available data. Furthermore, it is imperative to assess the efficacy of extant cybersecurity protocols and investigate the legislative frameworks that may influence fintech innovation. It is still unclear how financial literacy affects people's views of security and trust, particularly when it comes to the use of fintech and digital banking. Filling in these gaps will improve knowledge of the intricacies of financial technology, cybersecurity, and mobile banking in the Philippine setting.

IV. RESEARCH METHODOLOGY

In this chapter, it discusses the methods employed for collecting and analyzing data. It includes an explanation of the research design the individuals who participated in the study the tools utilized the steps taken during data collection and the statistical analysis conducted.

Research Design : This study assessed the relationship between cybersecurity challenges and BPI clients' adoption of modern banking procedures at the Biñan and San Pedro branches using a descriptive correlational methodology within a quantitative framework. The descriptive correlational design focuses on the relationships between these variables in addition to describing their current state. Finding patterns, evaluating correlations, and delving deeper into the relationships between variables like cybersecurity knowledge, frequency of financial technology use, and perceived risks are all made possible with this technique. A carefully chosen sample of clients will be given structured questionnaires to complete to gather as much information as possible about their perspectives and experiences with cybersecurity challenges and the use of financial technology.

Respondents of the Study : The research carefully determines its participants from the customer base of the Bank of the Philippine Islands (BPI) in Biñan and San Pedro Laguna. This study is conducted during the academic year 2023-2024. A sample size of 50 was determined from the total population. Quota sampling is a method of non-probability sampling where samples are selected based on the probability proportionate to the distribution of a variable in the population (Rukmana, 2014). This approach allows the research to encompass a broad spectrum of viewpoints, enhancing our comprehension of the relationship between cybersecurity protocols and bank customers' adoption of financial technology.

Sampling Procedure : To ensure a balanced representation of the various customers, a representative subset of BPI clients from the Biñan and San Pedro branches was carefully gathered for the study using quota sampling. A quota is set to guarantee that each segment of the population is sufficiently represented in the sample in quota sampling, a non-probability sampling technique in which the population is divided into discrete groups. The rationale behind using this particular method is its ability to accurately reflect the demographic characteristics of the sample, which in turn improves the findings' applicability and precision.

The target demographic is the Bank of the Philippine Islands customers in the Cavite South Laguna region, which includes the Biñan Pavilion Mall, Biñan Capinpin, Biñan Bonifacio, Biñan Southwoods Mall, San Pedro Pacita, and San Pedro branches. For this study, fifty clients—a mix of those from Binan and San Pedro—will be chosen. By ensuring that every branch is fairly represented in the sample, this technique offers a thorough overview of the experiences and viewpoints of the clients in various regions.The quota sampling approach is beneficial since it enables a systematic and fair representation of clients from each branch, guaranteeing that the results are impartial and representative of the total clientele. To correlate the sample with the real distribution of clients and enhance the study's validity and applicability to the larger population of BPI clients, participants were selected by specified quotas established for each branch.

Instrumentation and Validation : The self-made questionnaire underwent rigorous validation, including expert review by field specialists, ensuring its relevance and accuracy in capturing essential data for the research study which seeks to examine the cybersecurity challenges and financial technology adoption faced by BPI clients at the Biñan and San Pedro branches. A 4-point Likert scale for detailed responses was utilized, and the first section explored how clients perceive BPI's cybersecurity challenges. In the second section, the technology innovation was measured. A pilot test with a small number of BPI clients is carried out before the survey is fully implemented.

Evaluation and Scoring : The table below was used for the evaluation and scoring of the instrument to determine the Level of Cybersecurity Challenges.

Score	**Numerical Range**	**Categorical Response**	**Verbal Interpretation**
4	3.50- 4.00	Strongly Agree	Highly Experienced
3	2.50- 3.49	Agree	Experienced
2	1.50- 2.49	Disagree	Sometimes Experienced
1	1.0-1.49	Strongly Disagree	Not Experienced

The table below was used for the evaluation and scoring of the instrument to determine the Level of Financial Technology Adoption in Online Banking.

Score	Numerical Range	Categorical Response	Verbal Interpretation
4	3.50- 4.00	Strongly Agree	Highly Adopted
3	2.50- 3.49	Agree	Adopted
2	1.50- 2.49	Disagree	Moderately Adopted
1	1.0-1.49	Strongly Disagree	Not Adopted

Data Gathering Procedure : The researcher provided a consent form to both the company and the respondents, detailing the objectives and procedures of the online survey. This document sought permission for the respondents to participate in the survey and emphasized the voluntary nature of their involvement. This dual strategy guarantees greater involvement and respondent convenience. It is supported by the work of statisticians such as Florence Nightingale, who highlighted the significance of adaptable data collection methodologies. The in-person approach occurred in the Biñan and San Pedro branches, enabling face-to-face communication and prompt action. Simultaneously, the questionnaires are accessible online for individuals who would instead participate digitally, expanding the study's scope and inclusion.

Statistical Treatment of Data : The following statistical tools were used to analyze the research questions such as frequency and percentage distribution, weighted mean, and person r. The mean, or average, is the sum of all the data points in a set divided by the total number of data points (Turner, 2013). Using this measure of central tendency, SOP 1 and 2, the researcher will use a 4-point Likert scale to summarize the respondents' ratings of the clients' cybersecurity challenges and financial technology adoption of BPI.

Ethical Considerations : Throughout the investigation, the researcher carefully followed ethical standards. Formal authorization was acquired from the managers of the chosen Biñan and San Pedro BPI branches to collect data. Informed permission letters outlining the goals, methods, and respondent rights were given to BPI clients who will participate in the survey. These rights included the ability to remain anonymous, the ability to participate voluntarily, and the freedom to withdraw their participation at any moment. Additionally, participants were free to choose not to respond to any questions that would make them uncomfortable.

Participants were informed of the anticipated length of the survey and how their data would be used to guarantee ethical compliance in in-person and online survey methods. Clear guidelines and permission procedures will be established on the digital platform for the online survey. Participants are guaranteed access to the results once it is over, and they may check them over and ask for changes or omissions to protect their privacy and preferences. These steps were done to preserve the study's integrity and safeguard each participant's rights and welfare.

V. PRESENTATION, INTERPRETATION, AND ANALYSIS OF DATA

The interpretation and analysis of the data collected to address the study's research problems are presented in this chapter. The discussion proceeds according to the order in which the problem statement is presented in the first chapter.

The level of cybersecurity challenges experienced by bank clients : The objective of this study is to determine the level of cybersecurity challenges in terms of Phishing Attempts, Credential Stealing, and Account Takeover.

Table 1.1
Cybersecurity Challenges in Terms of Phishing Attempts.

Indicators	Mean	Verbal Interpretation	Rank
1. Sometimes I come across fake websites or links that look a lot like the official site of my bank. This could cause me to get confused and pose a security risk.	2.46	E	2
2. I often get emails or texts from people I don't know asking for private information like account numbers or passwords, saying they are from my bank.	2.72	HE	1
3. I've had problems or delays getting my bank's customer service or security team to fix security issues.	2.1	SE	4
4. I'm not sure if the security steps my bank has put in place to protect my personal and financial information are working.	2.42	SE	3
5. There have been purchases or activities that don't seem right in my bank account, which could be signs of fraud or a security breach.	1.86	SE	5
Average Weighted Mean	2.31	E	
Legend: 3.50-4.00 Highly Experienced (HE) 2.50-3.49- Experienced (E) 1.50 -2.49 Sometimes Experienced (SE) 1-1.49 Not Experienced (NE)			

Table 1.1 revealed the highest weighted mean of 2.72 was the indicator " I often get emails or texts from people I don't know asking for private information like account numbers or passwords, saying they are from my bank" and the lowest weighted mean of 1.86 was indicator " There have been purchases or activities that don't seem right in my bank account, which could be signs of fraud or a security breach." To sum up the average weighted mean is 2.31 verbally interpreted as **"Experienced**" This means that the attackers are using advanced strategies. To make their communications seem authentic, they could include official-looking logos, convincing wording, or even fictitious email accounts. They may also use social engineering strategies to instill panic or a sense of urgency, which would force listeners to take action without first confirming the legitimacy of the information.

The level of cybersecurity challenges faced by bank clients, particularly concerning phishing attempts, has been extensively explored in recent academic research. Li and Liu (2021) undertook a comprehensive analysis delving into the intricate cyber threats confronting banking institutions. Their study underscored the alarming sophistication of phishing tactics wielded by malicious actors, highlighting the ever-evolving nature of these threats. Similarly, Trendmicro.com (2019) further substantiated these findings in their research, noting a discernible uptick in the frequency and complexity of phishing attempts targeting bank clients in recent years. Their analysis illuminated the relentless adaptability of cybercriminals, who continually refine their methods to exploit vulnerabilities in financial systems. Moreover, the imperative for bolstered cybersecurity measures was underscored by Cristian (2023) in their seminal study. They emphasized the pressing need for proactive strategies to counteract the escalating menace posed by phishing attacks on financial institutions and their clientele.

Table 1.2
Cybersecurity Challenges in Terms of Credential Stealing.

Indicators	Mean	Verbal Interpretation	Rank
1. I'm overwhelmed by the number of passwords I need to remember for online services, including banking, which increases credential theft risk.	2.82	E	3
2. I have seen changes made without my permission to my account settings or personal information. This could mean someone else got in without my consent because my credentials were stolen.	2.14	SE	5
3. There have been times when someone got my login information and used it to get into my bank account without my permission.	3.08	E	1

4. Recovering from a credential theft event is a time-consuming and inconvenient process that involves changing passwords and checking transactions.	2.56	E	4
5. I'm not sure how safe it is for third-party apps or services that connect to my bank account to store my login information.	2.92	E	2
Average Weighted Mean	2.70	E	
Legend: 3.50-4.00 Highly Experienced (HE) 2.50-3.49- Experienced (E) 1.50 -2.49 Sometimes Experienced (SE) 1-1.49 Not Experienced (NE)			

Table 1.2 revealed the highest weighted mean of 3.08 was the indicator of "There have been times when someone got my login information and used it to get into my bank account without my permission" and the lowest weighted mean of 2.14 was the indicator of "I have seen changes made without my permission to my account settings or personal information. This could mean someone else got in without my consent because my credentials were stolen." To sum up the average weighted mean is 2.70 verbally interpreted as **"Experienced**" This means credential theft appears to be a significant issue, especially when it comes to bank account access, according to the data. While modifications to personal information or account settings are less frequent, they nonetheless raise concerns. Unauthorized entry is a big issue when it occurs frequently. These findings underscore the pressing need for enhanced security measures to mitigate the risk of unauthorized access and data breaches. Addressing these challenges is crucial for bolstering trust and confidence in online banking systems.The cybersecurity issues found fit with more general patterns that have been documented in previous research. One example of the frequency of unauthorized access concerns is the 72% of firms surveyed by Cybersecurity Insiders that reported an increase in account takeover threats (Cybersecurity Insiders, 2023). Concerns about third-party integration security are also in line with research from the Ponemon Institute, which showed that 60% of businesses had a data breach brought on by a third-party vendor (Ponemon Institute, 2022). Furthermore, the difficulty in keeping track of several passwords is consistent with the opinions expressed by LastPass's survey respondents, of whom 59% acknowledged sharing passwords between other accounts, hence increasing the possibility of credential theft (Fremery,2021).

Table 1.3
Cybersecurity Challenges in Terms of Account Takeover.

Interpretation	Mean	Verbal Interpretation	Rank
1. The convenience of accessing banking services through multiple devices and platforms increases the risk of unauthorized access to my accounts.	3.1	E	1
2. The lack of timely notification from my bank about suspicious activity or potential account takeover incidents undermines my confidence in their security measures.	2.98	E	2
3. Seeking to reclaim access to my accounts after an account takeover event was a frustrating process due to the slow response times and bureaucratic difficulties.	2.76	E	5
4. Regular security updates and fixes for online banking systems make them more likely to be used by fraudsters who want to get into accounts without permission.	2.84	E	4
5. The increasing number of data breaches in numerous businesses raises the possibility of my personal information being revealed, making it easier for hackers to stage account takeovers.	2.9	E	3
Average Weighted Mean	2.92	E	
Legend: 3.50-4.00 Highly Experienced (HE) 2.50-3.49- Experienced (E) 1.50 -2.49 Sometimes Experienced (SE) 1-1.49 Not Experienced (NE)			

Table 1.3 revealed the highest weighted mean of 3.1 was the indicator "The convenience of accessing banking services through multiple devices and platforms increases the risk of unauthorized access to my accounts" and

the lowest weighted mean of 2.76 was the indicator “Seeking to reclaim access to my accounts after an account takeover event was a frustrating process due to the slow response times and bureaucratic difficulties.” To sum up the average weighted mean is 2.92 verbally interpreted as **“Experienced**” This means that the difficulty of recovering access after account takeover incidents further emphasizes how serious the problem is. All things considered; increased protection is required to thwart unwanted access to bank accounts.

Supporting these findings, recent studies have emphasized the escalating threat landscape of account takeover incidents. For instance, the Identity Theft Resource Center reported a 72% increase in such incidents over the past year (Alder, S. (2024). Kisters, (2023) emphasizes the growing prevalence of cybersecurity threats in our interconnected world. He highlights the importance of taking proactive steps to safeguard personal data amidst rising incidents of hacking, ransomware, and other malicious attacks. Sharma, L. (2024) underscores the significance of regular software and device updates as a vital measure in maintaining robust cybersecurity defenses. Furthermore, these updates are essential for staying ahead of cybercriminals who constantly evolve their tactics, ensuring that any discovered security vulnerabilities are promptly addressed. Additionally, updates often introduce new features and enhance performance, their primary purpose is to bolster security and protect users' data.

2. The Level of Financial Technology Adoption on Online Banking: The objective of this study is to determine the level of financial technology in terms of digital payment and transfer using mobile wallets, peer-to-peer, and, robo advisors applications.

Table 2.1

Financial Technology Adoption in terms of Digital Payment and Transfer using Mobile Wallets.

Indicators	Mean	Verbal Interpretation	Rank
1. The bank has confidence in the security and reliability of mobile wallet transactions for digital payments conducted through online banking.	3.44	A	3
2. The bank values the effectiveness of customer support services in addressing queries or issues related to mobile wallets within online banking.	3.26	A	4
3. The bank understands and prioritizes customers' concerns about the security of their personal and financial information when using mobile wallets for digital transactions within online banking.	3.22	A	5
4. The bank is enthusiastic about exploring and implementing emerging features or technologies that enhance the functionality of mobile wallets within online banking, catering to our customers' evolving needs and preferences.	3.5	HA	2
5. The bank advocates for online banking platforms to provide educational programs aimed at enhancing users' awareness of safe and effective mobile wallet usage, promoting financial literacy and security among our customers.	3.68	HA	1
Average Weighted Mean	3.42	HA	
Legend: 3.50-4.00 Highly Adopted (HA) 2.50-3.49- Adopted (A) 1.50 -2.49 Moderately Adopted (MA) 1-1.49 Not Adopted (NA)			

Table 2.1 revealed the highest weighted mean of 3.68 was the indicator “ The bank advocates for online banking platforms to provide educational programs aimed at enhancing users' awareness of safe and effective mobile wallet usage, promoting financial literacy and security among our customers” and the lowest weighted mean of 3.22 was indicator “ The bank understands and prioritizes customers' concerns about the security of their personal and financial information when using mobile wallets for digital transactions within online banking..” To sum up the average weighted mean is 3.42 verbally interpreted as “**Highly Adopted**” This means that financial technology is widely used, especially for digital payments and transfers made with mobile wallets. Proactive behavior is demonstrated by the bank's support of educational initiatives aimed at raising user knowledge and giving priority to consumer concerns about security. Innovative digital payment solutions are being embraced in a positive trend, as seen by the high degree of adoption observed in these domains. A study

by Bashir et.al (2023) emphasizes the significance of educational initiatives in promoting consumer confidence and adoption of digital payment solutions. Similarly, a report by McKinsey emphasizes the critical role of technological innovation in meeting evolving customer needs and expectations in banking Haines, C. (2022). Furthermore, research by the Jafri et.al (2023) underscores the importance of trust and security in driving consumer adoption of mobile payment technologies. These provide robust support for the prioritization of customer education, innovation, and trust-building efforts observed in the adoption of mobile wallet technology within online banking.

Table 2.2
Financial Technology Adoption in terms of Digital Payment and Transfer using Peer-to-Peer

Indicators	Mean	Verbal Interpretation	Rank
1. The bank observes that many customers regularly engage in Peer-to-Peer (P2P) transactions for digital payments and transfers through the online banking platform, indicating the widespread adoption of this convenient payment method.	3.44	A	5
2. The bank expresses interest in and values enhanced security measures, such as biometric authentication, for securing Peer-to-Peer (P2P) transactions within the online banking platform, prioritizing the protection of customer transactions and data.	3.6	HA	3
3. The bank holds expectations for future enhancements or features in Peer-to-Peer (P2P) transactions within the online banking platform, anticipating speed improvements and expanded functionalities to meet evolving customer needs and preferences.	3.68	HA	1
4. . The bank acknowledges that many customers find the user interface of their online banking platform to be user-friendly and convenient for making digital payments, enhancing their overall banking experience.	3.62	HA	2
5. The bank acknowledges that some customers show a preference for Peer-to-Peer (P2P) transactions over traditional transfer methods (e.g., wire transfers) within online banking, highlighting the convenience and efficiency of P2P transactions for their banking needs.	3.5	HA	4
Average Weighted Mean	3.57	HA	
Legend: 3.50-4.00 Highly Adopted (HA) 2.50-3.49- Adopted (A) 1.50 -2.49 Moderately Adopted (MA) 1-1.49 Not Adopted (NA)			

Table 2.2 revealed the highest weighted mean of 3.68 was the indicator " The bank holds expectations for future enhancements or features in Peer-to-Peer (P2P) transactions within the online banking platform, anticipating speed improvements and expanded functionalities to meet evolving customer needs and preferences." and the lowest weighted mean of 3.44 was indicator " The bank observes that many customers regularly engage in Peer-to-Peer (P2P) transactions for digital payments and transfers through the online banking platform, indicating the widespread adoption of this convenient payment method." To sum up the average weighted mean is 3.57 verbally interpreted as **"Highly Adopted**" This means to adapt to changing client needs, the bank plans to improve P2P transactions in the future. Despite this, a large number of users routinely use the online banking platform to conduct P2P transactions.

Lara et.al (2023) indicates that explore the factors influencing individuals' intentions to use peer-to-peer (P2P) mobile payment services, considering the relatively low adoption rates despite the ubiquity of mobile technology. Through a comprehensive literature review, the paper identifies key determinants of mobile payment adoption. Subsequently, logistic regression analysis reveals six significant variables affecting P2P payment intentions: ease of use, perceived risk, personal innovativeness, perceived usefulness, subjective norms, and perceived enjoyment. Acopiado et.al (2023) Businesses in the Philippines must go digital as a result of the economic recovery following the COVID-19 epidemic. Their business activities can carry on under the new normal thanks to this innovation. One of the frequently suggested company recovery strategies that the government supports is the use of digital payments.

Table 2.3
Financial Technology. Adoption in terms of Robo-advisors application

Indicators	Mean	Verbal Interpretation	Rank
1. The accessibility of Robo-advisors contributes to the convenience of managing financial transactions online.	3.3	A	1
2. The user interface and experience of Robo-advisors in online banking are intuitive and user-friendly.	3.24	A	2
3. The level of transparency in Robo-advisors' recommendations and actions within online banking is satisfactory.	3.14	A	4
4. The integration of artificial intelligence and machine learning in Robo-advisors positively influences my trust in online banking services.	3.2	A	3
5. Robo-advisors' applications have improved the speed and efficiency of financial transactions in online banking.	3.08	A	5
Weighted Mean	3.19	A	
Legend: 3.50-4.00 Highly Adopted (HA) 2.50-3.49- Adopted (A) 1.50 -2.49 Moderately Adopted (MA) 1-1.49 Not Adopted (NA)			

Table 2.3 revealed the highest weighted mean of 3.30 was the indicator " The accessibility of Robo-advisors contributes to the convenience of managing financial transactions online." and the lowest weighted mean of 3.08 was the indicator " Robo-advisors' applications have improved the speed and efficiency of financial transactions in online banking." To sum up the average weighted mean is 3.19 verbally interpreted as **"Adopted**" This means financial technology is being adopted more and more, especially in online banking where robo-advisor apps are integrated. The ease of doing financial transactions online is greatly enhanced by the availability of robo-advisors, which also speed up and improve transaction efficiency. The degree of acceptance of robo-advisor programs in online banking is generally seen as Adopted, indicating that consumers generally accept and make use of these tools and that there is an increasing dependence on technology to make financial management duties easier.

Sharma, N. (2024) emphasizes that Robo advisors feature a user-friendly interface (UI) for seamless interaction via web and mobile apps, collecting and managing user information efficiently. Their algorithmic engine applies modern portfolio theory and risk assessment to offer personalized investment advice, determining optimal asset allocation. Nakatsuma, T. (2021) portfolio management system executes these strategies, handling trades and monitoring performance. Security measures, including encryption and compliance features, safeguard user data and assets. While largely automated, robo-advisors often provide customer support and educational resources, from FAQs to access to human advisors, enhancing user experience and comprehension.

Table 3.1 Test of Significant Relationship between the Level of cybersecurity challenges experienced by bank clients and financial technology adoption in online banking.

Table 3
Test of Significant Relationship Between Cybersecurity Challenges and Financial Technology Adoption

Cybersecurity Challenges	Financial Technology Adoption	r Value	p-value	Remarks	Description
Phishing Attempt	Mobile Wallet	-0.129	0.37195	Not Significant	Accept Ho
	Peer-to-peer	-0.183	0.20283	Not Significant	Accept Ho
	Robo-advisors applications	0.055	0.70622	Not Significant	Accept Ho
Credentials Stealing	Mobile Wallet	0.033	0.81811	Not Significant	Accept Ho
	Peer-to-peer	0.027	0.85415	Not Significant	Accept Ho
	Robo-advisors applications	0.201	0.16132	Not Significant	Accept Ho
	Mobile Wallet	0.093	0.52017	Not Significant	Accept Ho

Account Takeover	Peer-to-peer	0.042	0.77083	Not Significant	Accept Ho

Bank Security Measures

Cybersecurity Challenges	**Preventive Measures**	**Detective Measures**	**Corrective Measures**
Phishing Attempt	Regular cybersecurity training sessions are held by banks to inform staff members about potential dangers such as phishing scams and social engineering techniques. By increasing knowledge and encouraging best practices, staff members become more watchful and capable of identifying and handling security threats.	Employ cutting-edge email filtering systems to instantly identify and stop phishing emails before they are received by users. Suspicious trends can also be found by keeping a close eye on incoming email correspondence. Install systems that examine transaction patterns and user behavior to find any odd or suspicious activities that might point to a phishing attempt or compromised account.	Banks conduct post-event assessments and analyses to draw lessons from security breaches and pinpoint areas in need of development. Banks may adjust to changing cybersecurity issues and better safeguard their assets and clients by implementing regular security measure enhancements, revising policies and processes, and keeping up with emerging threats.
Credentials Stealing	Sensitive data, such as financial transactions and customer information, is protected by encryption in banks, whether it is being transferred over networks or kept in databases. This procedure ensures that the data is secure and confidential even if it is intercepted by rendering it unreadable to anyone lacking the necessary authorization.	The bank's security measures include the implementation of systems to track user login patterns, device fingerprints, and other activities to identify abnormalities that could point to unlawful access or credential theft. Through the examination of these data points, the bank can spot anomalies like strange device usage or unexpected logins, which allows them to react quickly to any security risks. The bank's cybersecurity posture is strengthened by this proactive approach, which immediately addresses new risks and protects sensitive assets from illegal access or data breaches.	Banks perform forensic investigations following a security incident to identify the underlying cause, evaluate the degree of damage, and get information for legal or regulatory requirements. Banks can use forensic analysis to better understand how the breach happened and put precautions in place to stop it from happening again.
Account Takeover	To enhance security, multi-factor authentication (MFA) requires users to supply more information than simply their password to access their accounts and complete transactions. Usually, it combines something the person has—like a smartphone or physical token—with something they know—like a password—or something they are—like a fingerprint or other biometric information. MFA improves overall	Implement AI-driven anomaly detection systems that watch user behavior and transactional activity all the time to identify trends that deviate from the norm and could be signs of attempted account takeover. Establish automated alerts to let security teams know about unauthorized access attempts or questionable login activity so they can look into it quickly and take appropriate action.	The recovery of hacked accounts requires strong support and unambiguous instructions from financial institutions, which are critical components of any customer service plan. In the case of a security breach or suspected illegal access, users require easily understandable instructions on how to quickly and efficiently retake control of their accounts. This assistance could come in the form of detailed instructions for changing passwords, stopping transactions to stop

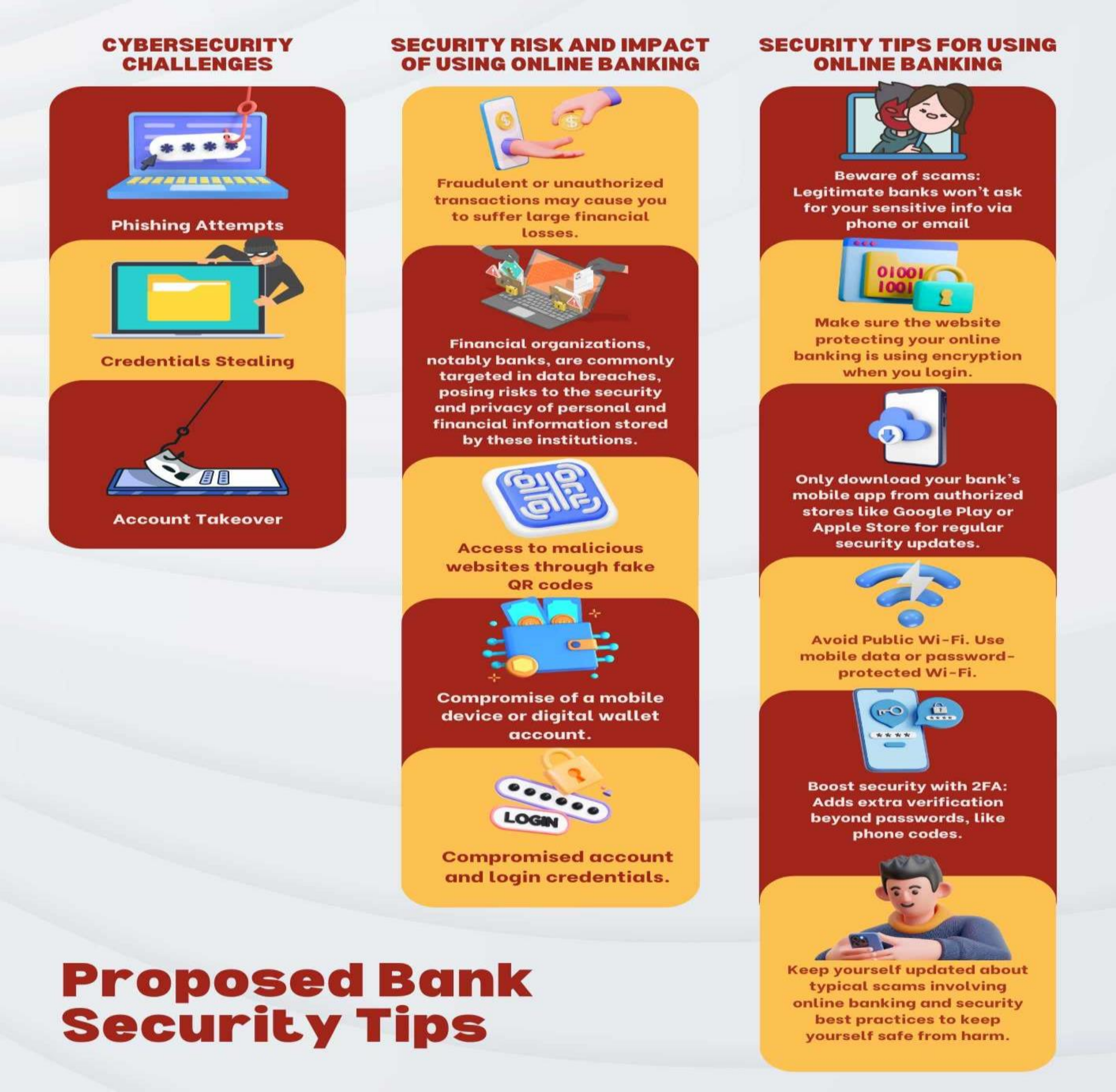
	account security by making it far more difficult for unauthorized people to access sensitive data or carry out fraudulent activities by demanding several forms of verification.		more illegal conduct, or starting fraud investigations to minimize any possible financial damages. It is important to have open lines of contact with consumers during these procedures, both online and off, so they feel encouraged and equipped to take the required precautions to safeguard their financial assets.

Table 4 Bank Security Measures

Banks use a range of preventive techniques to improve cybersecurity. Frequent staff training sessions help employees recognize and successfully respond to security threats by increasing their understanding of phishing scams and social engineering techniques. Sensitive information is shielded with encryption both during transmission and storage, guaranteeing its privacy even if it is intercepted. Furthermore, multi-factor authentication (MFA) strengthens security by requiring several verification methods, like passwords, biometrics, or tangible tokens. This makes it more difficult for unauthorized users to access accounts or carry out fraudulent operations.

Banks deploy detective techniques such as sophisticated email filtering to stop consumers from receiving phishing emails and tracking incoming email traffic for unusual patterns. The analysis of transaction patterns and user behavior looks for anomalies that might point to hacked accounts or possible phishing attempts. To detect anomalies and enable timely reaction to security threats, systems monitor login patterns, device fingerprints, and other activity. While automated warnings tell security teams of unauthorized access attempts or questionable login activity so they may take immediate action, AI-driven anomaly detection systems continuously monitor user behavior and transactional activity to discover trends deviating from the usual.

In the aftermath of security breaches, banks enhance security protocols, update policies, conduct incident assessments to learn from them, and adopt corrective actions. To find the sources of breaches, evaluate the harm, and satisfy legal requirements, forensic investigations are conducted. Account recovery requires a banking institution's strong cooperation and unambiguous instructions, which include changing the password, stopping transactions, and starting a fraud inquiry. Customers who feel empowered to safeguard their financial assets are guaranteed by open lines of contact.



CYBERSECURITY CHALLENGES

Phishing Attempts

Credentials Stealing

Account Takeover

SECURITY RISK AND IMPACT OF USING ONLINE BANKING

Fraudulent or unauthorized transactions may cause you to suffer large financial losses.

Financial organizations, notably banks, are commonly targeted in data breaches, posing risks to the security and privacy of personal and financial information stored by these institutions.

Access to malicious websites through fake QR codes

Compromise of a mobile device or digital wallet account.

Compromised account and login credentials.

SECURITY TIPS FOR USING ONLINE BANKING

Beware of scams: Legitimate banks won't ask for your sensitive info via phone or email

Make sure the website protecting your online banking is using encryption when you login.

Only download your bank's mobile app from authorized stores like Google Play or Apple Store for regular security updates.

Avoid Public Wi-Fi. Use mobile data or password-protected Wi-Fi.

Boost security with 2FA: Adds extra verification beyond passwords, like phone codes.

Keep yourself updated about typical scams involving online banking and security best practices to keep yourself safe from harm.

Proposed Bank Security Tips

Table 5. Bank Security Tips

Users may experience negative effects and serious security hazards when using online banking. Transactions that are unlawful or fraudulent might cost a significant amount of money. Data breaches frequently target financial institutions, most notably banks, exposing consumers' private and sensitive financial information to possible exposure. Malicious NFC tags and QR codes are a serious risk because they can accidentally direct users to dangerous websites and expose them to a range of unfavorable outcomes. Furthermore, thieves may be able to access banking information without authorization using compromised mobile devices or digital wallet accounts. Attacks using malware and phishing techniques are still common, giving hackers access to login credentials and the ability to carry out fraudulent transactions under pretenses. These dangers highlight the necessity of strong security protocols and user awareness when using the Internet for banking.

Being alert to fraudulent efforts to obtain your banking details by phone calls, text messages, or emails is crucial for ensuring secure online banking. PINs and passwords are not requested through these channels by reputable banks. Check for the presence of a padlock icon in the address bar and "https://" in the URL when connecting to your online banking account to ensure that the website is encrypted. Downloading your bank's mobile banking app from official app stores—like the Apple App Store or Google Play—will guarantee legitimacy and timely security updates. Financial transactions should not be conducted over public Wi-Fi networks due to security concerns. Choose a safe, password-protected Wi-Fi network or your mobile data instead. By setting two-factor authentication (2FA), which calls for a second form of verification—such as a code texted to your phone—you can increase security. Keep yourself updated about typical scams involving online banking and security best practices to keep yourself safe from harm. Staying up to date with emerging trends enables you to protect your financial assets and remain one step ahead of fraudsters.

VI. SUMMARY, CONCLUSION, AND RECOMMENDATION

This chapter thoroughly summarizes the study's major conclusions and how they relate to the issue. It summarizes the key findings, analysis conclusions, and recommendations based on the findings of the statistical tests carried out.

Summary of findings

1. The level of cybersecurity challenges experienced by bank clients in terms of phishing attempts revealed a mean of 2.31; in terms of credential stealing, 2.70; and in terms of account takeover, 2.91.
2. The level of financial technology adoption in terms of digital and payment-using mobile wallets revealed a mean of 3.42, in terms of digital and payment-using peer-to-peer, 3.56, and, in terms of robo-advisors application, 3.19.
3. The probability values are all greater than the level of significance at .05 thus, accept the null hypothesis (Ho).
4. Overall, it seems that a large number of bank customers are not sufficiently informed on cybersecurity precautions. Their lack of knowledge makes them susceptible to several types of online attacks and undermines their capacity to properly protect their financial resources.

Conclusions

After presenting the findings of the study, the following conclusions were drawn:

1. The level of cybersecurity challenges in terms of phishing attempts, credentials stealing, and, account takeover were all rated experienced. Attackers are using advanced techniques, such as social engineering and official-looking features, to trick users into disclosing private information or acting right away. The frequency of credential theft highlights a serious security risk, especially when it comes to bank account access. Changes to account settings or personal information, albeit less common, also cause concern. Increased security measures must be put in place since frequent unlawful entrance increases the danger of data breaches.
2. The level of financial technology adoption in terms of digital payment and transfer using mobile wallets and peer-to-peer are rated as Highly Adopted while the robo-advisors application is rated as adopted. Financial technology is widely used, especially when it comes to digital payments and transfers via mobile wallets. A good trend toward raising user knowledge and safety is seen in the bank's proactive support of educational programs and prioritizing consumer security issues. Innovative digital payment solutions are also being well received in the market, as seen by the high adoption rates of these systems. Peer-to-peer (P2P) transactions are primarily conducted through online banking. To accommodate consumer preferences and behaviors, financial technology is always evolving. The growing use of financial technology is evident in online banking, where robo-advisor apps are integrated to improve transaction efficiency and convenience. The increasing adoption of robo-advisor programs indicates the banking industry's move toward deeper technological integration and a rising dependence on technology to simplify financial management responsibilities.
3. The use of financial technology in online banking and cybersecurity issues are not significantly related. The study indicates that cybersecurity difficulties do not considerably influence financial technology adoption, as evidenced by non-significant p values, despite weak relationships between cybersecurity challenges and various forms of financial technology. For the banking industry, cybersecurity is still essential, and continuous efforts are required to reduce risks and guarantee safe online transactions. Safeguarding confidential financial data and preserving confidence in digital financial services need proactive responses to cybersecurity risks.
4. Robust security measures must be implemented due to the enormous cybersecurity threats that come with the increasing adoption of financial technology. Banks may successfully secure their digital infrastructure and shield their clients from ever-evolving cyber dangers by recommending and implementing thorough security measures.

Recommendations

From the findings and conclusions, the researcher recommends the following:

1. The implementation entails promoting regular software and hardware upgrades to address security

vulnerabilities, implementing multi-factor authentication (MFA) and other strong authentication approaches, and educating customers about common threats including malware, phishing, and social engineering. In addition, banks will promote safe banking apps, fraud detection services, secure communication channels, and a strong password policy. The bank will also provide monitoring tools to identify any strange activity. To further create a safer environment for banking operations and customer interactions, continuing cybersecurity awareness initiatives and conveniently accessible customer support will be put into place. This proactive strategy highlights the significance of enlightening clients about possible cyber threats and giving them the tools they need to successfully safeguard their financial information.

2. The bank has to raise awareness, improve accessibility and usability, give security measures top priority to build confidence, combine fintech with traditional banking services seamlessly, and innovate constantly to meet changing client needs to promote the adoption of financial technology. These programs seek to improve financial inclusion and customer empowerment by utilizing efficient and secure digital financial management technologies.

3. The bank must prioritize cybersecurity even though the study found that cybersecurity risks do not greatly impact financial technology adoption in online banking. The tenuous connections between different cybersecurity threats and financial technology types highlight the necessity of ongoing attention to detail. To reduce cybersecurity risks, banks should take a proactive approach. This includes implementing advanced security processes, doing routine security audits, and keeping up with new threats. It's also critical to remind consumers about safe internet behavior and the value of protecting their data. Banks can protect sensitive financial information, guarantee secure online transactions, and uphold consumer confidence in digital financial services by implementing strong cybersecurity measures.

4. To successfully execute bank security measures, financial institutions had to use a multifaceted approach encompassing new technologies, personnel education, and client outreach. This includes doing frequent security audits, incorporating security technology like multi-factor authentication and AI-based fraud detection, and giving staff members cybersecurity training. Banks should also instruct their clients on how to safeguard their accounts by using strong passwords and spotting phishing scams. Banks can improve security, safeguard their digital infrastructure, and win over customers by using these strategies.

5. Future studies have to focus more on comprehending the intricate relationship between cybersecurity risks and financial technology usage. To investigate the complex variables influencing user behavior and technology adoption over time, longitudinal research, mixed-method techniques, and varied demographic analyses are advised. Further research into the efficacy of cybersecurity protocols and customer education initiatives might provide insightful information to banks looking to strengthen their security systems. The results of this study will advance our knowledge of how to balance the advancement of financial technology with strict cybersecurity procedures.

REFERENCES

1. Aji, H. M., Berakon, I., & Husin, M. M. (2020). COVID-19 and e-wallet usage intention: A multigroup analysis between Indonesia and Malaysia. Cogent Business & Management, 7(1), 1–16.
2. Al Ali, L., Jagal, J., Joseph, J., Ahmed, I. S., & Rawas--Qalaji, M. (2022). Pharmaceutical equivalency of locally and regionally manufactured generic pharmaceutical products in UAE. Saudi Pharmaceutical Journal.
3. Al--Shbiel, S. O., & Ahmad, M. A. (2018). A theoretical discussion of electronic banking in Jordan by integrating technology acceptance model and theory of planned behavior. International Journal of Academic Research in Accounting, Finance and Management Sciences, 6(3), 272--284
4. Al-Somali, S. A., Gholami, R., & Clegg, B. (2018). An investigation into the acceptance of online banking in Saudi Arabia. Technovation, 29(2), 130-141.
5. Alam, Md. M., & Dangarwala, Dr. U. R. (2020). Internet Banking Customer Satisfaction and Online Banking Service Attributes. Indian Journal of Applied Research, 1(6), 198–199. https://doi.org/10.15373/2249555x/mar2020/66
6. Ali, M., Raza, S. A., Puah, C. H., & Amin, H. (2019). Consumer acceptance toward takaful in Pakistan: An application of diffusion of innovation theory. International Journal of Emerging Markets.
7. Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. International Journal of Information Management, 53.
8. Amora, J., Ochoco, M., & Anicete, R. (2016). Student engagement and college experience as the mediators of the relationship between institutional support and academic performance. Digital Journal

of Lasallian Research, (12), 15–30.

9. Andriani, P., Setyorini, N., & Shibghatalloh, A. (2021). Investigating e-servicescape influence to customer response in digital islamic banking. International Journal of Islamic Economics and Finance (Ijief), 4(1). https://doi.org/10.18196/ijief.v4i1.10299
10. Ariyani, E. and Junaidi, J. (2022). Position and evidence of predicate crime in the crime of money laundering. Proceedings of the 1st International Seminar on Sharia, Law and Muslim Society (ISSLAMS 2022), 108-116. https://doi.org/10.2991/978-2-494069-81-7_13
11. Arman, M. (2023). Money laundering: a three-step secret game. Advanced Qualitative Research, 1(1), 30-41. https://doi.org/10.31098/aqr.v1i1.1280
12. Ashta, A. and Herrmann, H. (2021). Artificial intelligence and fintech: an overview of opportunities and risks for banking, investments, and microfinance. Strategic Change, 30(3), 211-222. https://doi.org/10.1002/jsc.2404
13. Basit, A., Zafar, M. Q., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2020). A comprehensive survey of ai-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1), 139-154. https://doi.org/10.1007/s11235-020-00733-2
14. Beu, N., Jayatilaka, A., Zahedi, M., Babar, M., Hartley, L., Lewinsmith, W., … & Baetu, I. (2022). Falling for phishing attempts: an investigation of individual differences that are associated with behavior in a naturalistic phishing simulation.. https://doi.org/10.31234/osf.io/xdk53
15. Bokhari, S. A. A. (2022). Factors influencing implementation of cybersecurity laws in developing economies: evidence with quantitative analysis from Pakistan.. https://doi.org/10.31124/advance.20066321
16. Cahaya, Y. F., Mursitama, T. N., Hamsal, M., & Tjhin, V. U. (2023). Increasing e-loyalty of banking customers through customer trust and commitment. International Journal of Applied Economics, Finance and Accounting, 15(2), 96-104. https://doi.org/10.33094/ijaefa.v15i2.844
17. Chaki, S. M. H., Din, M. M., & Siraj, M. M. (2019). Integration of sql injection prevention methods. International Journal of Innovative Computing, 9(2). https://doi.org/10.11113/ijic.v9n2.232
18. Chamlongrath, W., & Tingsabhat, C. The Payment Behavior and Electronic Payments Usage of University Students.
19. Cherkasova, M. (2021). Theoretical fundamentals of strategy and strategic management in banking sphere. Socio-Economic Research Bulletin, (3-4(78-79)), 132-141. https://doi.org/10.33987/vsed.3-4(78-79).2021.132-141
20. Chin, W. W. (1998). The partial least squares approach to structural equation modeling. Modern methods for business research, 295(2), 295–336.
21. Chronopoulos, D. K., Lukas, M., & Wilson, J. O. S. (2020). Consumer spending responses to the Covid-19 pandemic: An assessment of Great Britain. SSRN Electronic Journal.
22. Cohen, J. (1988). Statistical power analysis for the behavioral sciences, Hillsdale, NJ: Lawrence Erlbaum.
23. Cunningham, L. F., Gerlach, J., & Harper, M. D. (2021). Perceived risk and e-banking services: An analysis from the perspective of the consumer. Journal of Financial services marketing, 10(2), 165-178
24. Dai, X., & Grundy, J. (2017). NetPay: An off-line, decentralized micro-payment system for thin-client applications. Electronic Commerce Research and Applications, 6(1), 91–101
25. Das, A., Baki, S., Aassal, A. E., Verma, R. M., & Dunbar, A. (2020). Sok: a comprehensive reexamination of phishing research from the security perspective. IEEE Communications Surveys &Amp; Tutorials, 22(1), 671-708. https://doi.org/10.1109/comst.2019.2957750
26. Elhajjar, S., & Ouaida, F. (2020). An analysis of factors affecting mobile banking adoption. International Journal of Bank Marketing, 38(2), 352-367.
27. Fairlie, R. W., Robb, A., & Robinson, D. T. (2022). Black and white: access to capital among minority-owned start-ups. Management Science, 68(4), 2377-2400. https://doi.org/10.1287/mnsc.2021.3998
28. Fang, Y.-H. (2018). Beyond the credibility of electronic word of mouth: Exploring eWOM Adoption on Social Networking Sites from Affective and Curiosity Perspectives. International Journal of Electronic Commerce, 18 67–102.
29. Fares, O. H., Butt, I., & Lee, S. H. M. (2022). Utilization of artificial intelligence in the banking sector: a systematic literature review. Journal of Financial Services Marketing, 28(4), 835-852. https://doi.org/10.1057/s41264-022-00176-7
30. Fornell C., & Larcker, D. F. (1981). Evaluating structural equation models with unobserved variables and measurement error. Journal of Marketing Research, 18(1), 39–50. http://doi.org/10.2307/3151312
31. Fornell, C. & Larcker, D. F. (1984). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39 – 50.

32. Gautam, R. S., & Kanoujiya, J. A. G. J. E. E. V. A. N. (2022). Role of Regional Rural Banks in Rural Development and Its Influences on Digital Literacy in India. Iconic Research and Engineering Journals, 5(12), 92-101.
33. Głodowska, A., Wach, K., & Maciejewski, M. (2023). Does high-tech industry matter for marketing strategy selection? adaptation vs. standardization on the international market. Studies of the Industrial Geography Commission of the Polish Geographical Society, 37(1). https://doi.org/10.24917/20801653.371.4
34. Govender, I., & Sihlali, W. (2020). A study of mobile banking adoption among university students using an extended TAM. Mediterranean journal of social sciences, 5(7), 451.
35. Hair, J. F., Anderson, R. E., & Tatham, R. L. (1987). Multivariate data analysis. New York, NY: Macmillan.
36. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2022). Multivariate data analysis. Upper Saddle River, NJ: Prentice Hall.
37. Hair, J. F., Ringle, C. M. & Sarstedt, M. (2020). PLS-SEM: Indeed, a silver bullet. Journal of Marketing Theory and Practice, 19(2), 139 – 151.
38. Hanafizadeh, P., & Khedmatgozar, H. R. (2020). The mediating role of the dimensions of the perceived risk in the effect of customers' awareness on the adoption of Internet banking in Iran. Electronic Commerce Research, 12(2), 151-175.
39. Hanafizadeh, P., Byron, W.K. & Khedmatgozar H.R. (2019). A systematic review of internet banking adoption Telematics and Informatics, 31, 492-510.
40. Hassandoust, F., Singh, H., & Williams, J. (2020). The role of contextualization in individuals' vulnerability to phishing attempts. Australasian Journal of Information Systems, 24. https://doi.org/10.3127/ajis.v24i0.2693
41. Holovkin, B., Tavolzhanskyi, O. V., & Lysodyed, O. (2021). Corruption as a cybersecurity threat in conditions of the new world's order. Linguistics and Culture Review, 5(S3), 499-512. https://doi.org/10.21744/lingcure.v5ns3.1538
42. Johri, A. and Kumar, S. (2023). Exploring customer awareness towards their cyber security in the kingdom of saudi arabia: a study in the era of banking digital transformation. Human Behavior and Emerging Technologies, 2023, 1-10. https://doi.org/10.1155/2023/2103442
43. Karagiannis, S., Magkos, E., Karavaras, E., Karnavas, A., Nikiforos, M. N., & Ntantogian, C. (2022). Towards nice-by-design cybersecurity learning environments: a cyber range for soc teams.. https://doi.org/10.21203/rs.3.rs-1902186/v1
44. Khan, A., Mubarik, M. S., & Naghavi, N. (2021). What matters for financial inclusions? evidence from emerging economy. International Journal of Finance &Amp; Economics, 28(1), 821-838. https://doi.org/10.1002/ijfe.2451
45. Kim, H. J., & Lee, J. M. (2022). The barriers and drivers of postponers' adoption intention of mobile-only banks. International Journal of Mobile Communications, 20(3), 309-331.
46. Kock, N. (2017). WarpPLS user manual: Version 6.0. ScriptWarp Systems: Laredo, TX, USA, 141.
47. Köhler, J., Raven, R., & Walrave, B. (2020). Advancing the analysis of technological innovation systems dynamics: Introduction to the special issue. Technological Forecasting and Social Change, 158, 120040. https://doi.org/10.1016/j.techfore.2020.120040
48. Koo, D. M., & Ju, S. H. (2020). The interactional effects of atmospherics and perceptual curiosity on emotions and online shopping intention. Computers in Human Behavior, 26(3), 377–388.
49. Kotler, P., & Armstrong, G. (2020). Principles of marketing. Pearson education. .
50. Kuzmenko, O., Pilina, N., & Pilin, R. (2020). Trends of fraud operations on the banking market and approaches of cybersecurity as-sessment. Efektyvna Ekonomika, (5). https://doi.org/10.32702/2307-2105-2020.5.11
51. Ladkoom, K., & Thanasopon, B. (2020, May). Factors Influencing Reuse Intention of e-Payment in Thailand: A Case Study of PromptPay. In ICEIS (1) (pp. 743-750).
52. Lee, J. C. and Chen, X. (2022). Exploring users' adoption intentions in the evolution of artificial intelligence mobile banking applications: the intelligent and anthropomorphic perspectives. International Journal of Bank Marketing, 40(4), 631-658. https://doi.org/10.1108/ijbm-08-2021-0394
53. Liébana, C. F., Muñoz, L. F., & Rejón, G. F. (2019). The determinants of satisfaction with e-banking Industrial Management & Data Systems, 113 (5), 750-767.
54. Lin, C., Liu, S., & Wei, L. (2022). Banking and innovation: a review. Journal of Chinese Economic and Business Studies, 21(1), 143-176. https://doi.org/10.1080/14765284.2022.2127397
55. Markard, J., Hekkert, M. P., & Jacobsson, S. (2015). The technological innovation systems framework: Response to six criticisms. Environmental Innovation and Societal Transitions, 16, 76–86.

https://doi.org/10.1016/j.eist.2015.07.006

56. Mbama, C. I., Ezepue, P., Alboul, L., & Beer, M. (2018). Digital banking, customer experience, and financial performance: UK Bank managers' perception. Journal of Research in Interactive Marketing, 12(4), 432–451.
57. Meuleman, B. (2020). Cross-cultural analysis. E. Davidov, P. Schmidt, & J. Billiet (Eds.). Routledge Academic.
58. Mohammadi, H. (2019). A study of mobile banking usage in Iran. International Journal of Bank Marketing, 33 (6). 733-759, doi.org/10.1108/IJBM-08-2019-0114.
59. Moodley, T., & Govender, I. (2017). Factors influencing academic use of internet banking services: An empirical study. African Journal of Science, Technology, Innovation and Development, 8(1), 43--51.
60. Munari, S. A. L. H., & Susanti, S. (2021). The Effect of Ease of Transaction, Digital Literacy, and Financial Literacy on The Use of E-Banking.Economic Education Analysis Journal,10(2), 298-309.
61. Mykhailiuk, G., Рустамзаде, А. Х. о., Mykhailiuk, N., & Zaitseva-Kalaur, I. (2021). Egulation and supervision of financial services in the era of global digitalization: experience of azerbaijan. Financial and Credit Activity Problems of Theory and Practice, 5(40), 28-34. https://doi.org/10.18371/fcaptp.v5i40.244860
62. Nguyen, B. (2021). Networking in weak institutions: when is it good for small business investment? the case of vietnam. Management and Organization Review, 18(3), 583-620. https://doi.org/10.1017/mor.2020.85
63. Nunnally, J. C. (1978). Psychometric theory. New York, NY: McGraw Hill.
64. Nunnally, J. C., & Bernstein, I.H. (1994). Psychometric theory. New York, NY: McGraw Hill.
65. Oh, K. Y., Cruickshank, D., & Anderson, A. R. (2019). The adoption of e-trade innovations by Korean small and medium sized firms. Technovation, 29(2), 110–121.
66. Ongore, V. O., & Kusa, G. B. (2018). Determinants of financial performance of commercial banks in Kenya. International journal of economics and financial issues, 3(1), 237-252.
67. Parkavi, B., & Rajkumar, S. (2022). CUSTOMERS PERCEPTION TOWARDS CRM PRACTICES ADOPTED BY PUBLIC SECTOR BANKS IN E-BANKING ERA.
68. Petrovna, E., Victorovna, O., & Aleksandrovna, O. Digitalization of banking business–actual development strategies. In IX INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE “MANAGERIAL SCIENCES IN THE MODERN WORLD” (p. 55).
69. Potia, A., & Dahiya, K. (2020). Optimistic, digital, generous: COVID-19’s impact on Indonesian consumer sentiment
70. Puchkova, N. (2019). Role of innovations in increase in efficiency of bank activity. Proceedings of the Internation Conference on "Humanities and Social Sciences: Novations, Problems, Prospects" (HSSNPP 2019). https://doi.org/10.2991/hssnpp-19.2019.168
71. Qin, R. (2021). Identification of accounting fraud based on support vector machine and logistic regression model. Complexity, 2021, 1-11. https://doi.org/10.1155/2021/5597060
72. Rabbani, M. R., Lutfi, A., Ashraf, M. A., Nawaz, N., & Watto, W. A. (2023). Role of artificial intelligence in moderating the innovative financial process of the banking sector: a research based on structural equation modeling. Frontiers in Environmental Science, 10. https://doi.org/10.3389/fenvs.2022.978691
73. Rachna, & Singh, P. (2018). Issues and Challenges of Electronic Payment Systems. International Journal for Research in Management and Pharmacy, 2(9), 25–30.
74. Rahim, M. and Basheer, K. P. M. (2021). A survey on anti-phishing techniques: from conventional methods to machine learning. Malaya Journal of Matematik, 9(1), 319-328. https://doi.org/10.26637/mjm0901/0054
75. Reljic, J., Cetrulo, A., Cirillo, V., & Coveri, A. (2021). Non-standard work and innovation: evidence from european industries. Economics of Innovation and New Technology, 32(1), 136-164. https://doi.org/10.1080/10438599.2021.1893139
76. Roldán, J. L., & Sánchez-Franco, M. J. (2020). Variance-based structural equation modeling: Guidelines for using partial least squares in information systems research. In Research methodologies, innovations and philosophies in software systems engineering and information systems (pp. 193-221). IGI Global.
77. Samašonok, K., Kamienas, E., & Juškevičienė, A. (2023). The use of biometric technologies in ensuring critical infrastructure security: the context of protecting personal data. Entrepreneurship and Sustainability Issues, 10(3), 133-150. https://doi.org/10.9770/jesi.2023.10.3(10)
78. Sazonov, S., Езангина, И. А., Polianskaia, A., & Chunakov, A. (2021). Digital transformation and its role in the reproduction of innovative development of the modern banking institution of russia. SHS

Web of Conferences, 114, 01009. https://doi.org/10.1051/shsconf/202111401009

79. Schierz, P. G., Schilke, O., & Wirtz, B. W. (2020). Understanding consumer acceptance of mobile payment services: An empirical analysis. Electronic Commerce Research and Applications, 9(3), 209–216.
80. Schierz, P.G., Oliver, S. & Bernd W.W. (2020). Understanding consumer acceptance of mobile payment services: An empirical analysis. Electronic Commerce Research and Applications, 9 (3), 209-216.
81. Shin, J. W. (2021). Mediating effect of satisfaction in the relationship between customer experience and intention to reuse digital banks in Korea. Social Behavior and Personality: an international journal, 49(2), 1-18.
82. Siddique, S., Yasmin, M., Taher, T., & Alam, M. (2021). The reliability and acceptance of biometric system in bangladesh: users perspective. International Journal of Computer Trends and Technology, 69(6), 15-21. https://doi.org/10.14445/22312803/ijctt-v69i6p103
83. Singh, G., & Pandey, A. (2022). Digital Banking for Rural Transformation a Comparative Study of Andhra Pradesh and Uttar Pradesh.
84. Sivaprakash, V. S. and Venkatesh, S. (2020). Customer satisfaction towards modern banking services of banks with special reference to vellore. International Journal of Engineering and Advanced Technology, 9(3), 2005-2006. https://doi.org/10.35940/ijeat.b3083.029320
85. Smith, A. (2018). Smartphone ownership-2019 update (Vol. 12, p. 2019). Washington, DC: Pew Research Center.
86. Sohns, F. and Wójcik, D. (2020). The impact of brexit on london's entrepreneurial ecosystem: the case of the fintech industry. Environment and Planning A: Economy and Space, 52(8), 1539-1559. https://doi.org/10.1177/0308518x20925820
87. Srivastav, A. and Vallascas, F. (2022). Small business lending and regulation for small banks. Management Science, 68(10), 7742-7760. https://doi.org/10.1287/mnsc.2021.4176
88. Teka, B. M. (2020). Factors affecting bank customers usage of electronic banking in Ethiopia: Application of structural equation modeling (SEM). Cogent Economics & Finance, 8(1), 1762285.
89. Teoh Teng Tenk M, Yew HC, Heang LT (2020). E-wallet Adoption: A case in Malaysia. International Journal of Research In Commerce and Management Studies. 216-233
90. Thakur, R. (2019). What keeps mobile banking customers loyal? International Journal of Bank Marketing, 32 (7), 628-646.
91. Tharani, J. S. and Arachchilage, N. G. A. (2020). Understanding phishers' strategies of mimicking uniform resource locators to leverage phishing attacks: a machine learning approach. Security and Privacy, 3(5). https://doi.org/10.1002/spy2.120
92. Tot, I., Bajčetić, J., Jovanović, B. Ž., Trikoš, M., Bogićević, D., & Gajić, T. M. (2021). Biometric standards and methods. Vojnotehnicki Glasnik, 69(4), 963-977. https://doi.org/10.5937/vojtehg69-32296
93. Vishwanath, M. (2023). Legal support of cybersecurity in the field of application of artificial intelligence technology &amp;amp; analysis for cybersecurity solutions in industry 4.0 platforms.. https://doi.org/10.31219/osf.io/6z79c
94. Wang, J., Xu, C., & Liu, W. (2022). Understanding the adoption of mobile social payment: from the cognitive behavioural perspective. International Journal of Mobile Communications, 20(4), 483-506.
95. Wasiul Karim Md, Haque A, Arije Ulfy Md, Alamgir Hossain Md, et al.: Factors Influencing the Use of E-wallet as a Payment Method among Malaysian Young Adults. Journal of International Business and Management. 2020; 3 (1).
96. Wiefling, S., Tolsdorf, J., & Iacono, L. L. (2021). Privacy considerations for risk-based authentication systems. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&amp;PW). https://doi.org/10.1109/eurospw54576.2021.00040
97. Xie, Y., Zhou, Y., Xu, J., Zhou, J., Chen, X., & Xiao, F. (2021). Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: state-of-the-art and future challenges. Software: Practice and Experience, 51(11), 2108-2127. https://doi.org/10.1002/spe.2965
98. Yasa, I. B. A., Sukayasa, I. K., & Utami, N. M. M. A. (2022). The influence of the bystander effect and internal control on the trend of accounting fraud at village credit institutions in jembrana regency. Proceedings of the International Conference on Applied Science and Technology on Social Science 2022 (iCAST-SS 2022), 53-56. https://doi.org/10.2991/978-2-494069-83-1_10
99. Yu, P.L., Balaji, M.S. & Khong, K.W. (2019). Building trust in internet banking: A trustworthiness perspective. Industrial Management & Data Systems, 115 (2), 235-252.
100. Yusoff, Y. H., Hamidi, A. S. W. M., Ali, N. A. C., Zaidi, N. F. M., Isa, N. S., & Paharazi, M. A. B. A.

(2023). Role of auditors in reducing effects of money laundering: concept paper. International Journal of Academic Research in Economics and Management Sciences, 12(1). https://doi.org/10.6007/ijarems/v12-i1/16585

101. Zhang, J., & Mao, E. (2022). Understanding the acceptance of mobile SMS advertising among young Chinese consumers. Psychology & Marketing, 25(8), 787