Journal of Business and Management Studies
ISSN: 2709-0876
DOI: 10.32996/jbms
Journal Homepage: www.al-kindipublisher.com/index.php/jbms

JBMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Security Measures Applied on Digital Banking Towards Service Improvement Proposal

LI FANG[1] and Darwin G. Quintos[2] ✉
University of Perpertual Help System Dalta
Corresponding Author: Darwin G. Quintos **E-mail**: dgquintos22@gmail.com

| ABSTRACT

The main objective of this study is to assess the security measures on digital banking as a basis for improving services. The researcher used a descriptive method of research, employed with the used of a standard questionnaire. Descriptive research design involves gathering data that seeks to describe events and then organizing, tabulates, depicts, and describes the data collection in a systematic manner. (Glass, G. V., & Hopkins, K. D. 1984) The survey questionnaire is divided into two parts: the demographic profile of respondents and the list of questions that the researcher aims to know in order to collect valid and reliable data needed for the study. The second part was subdivided into 3 parts, which are Security Measures on Digital Banking, Common Digital Banking Issues and Problems Encountered by Respondents, and an open-ended question about Suggestions & other problems encountered. The security measures on digital banking in terms of trust and security trust and security, knowledge and awareness, ease of use, and usefulness are strongly agreed upon. However, it is necessary to improve the security measures with regard to accessing the apps using multiple devices, securing one time passwords, an easy withdrawal system, and clearing service requests.

| KEYWORDS

Security Measures, Digital Banking, Ease to

| ARTICLE INFORMATION

ACCEPTED: 05 September 2023 **PUBLISHED:** 16 September 2023 **DOI:** 10.32996/jbms.2023.5.5.5

1. Introduction

The banking sector in a nation serves as the foundation upon which the pillars of economic growth and development can be built. In recent years, the digital economy has shaped unprecedented changes in global markets. The rapid growth of information technology and Information communication technology contributes significantly to the advancement of digital banking (Schreieck & Wiesche, 2017) and progressively transforms our day-to-day activities to become more reliant on these technologies. Digitization offers many benefits to core banking systems, notably in meeting the rising demands of retail and consumer banking clients in providing an automated service for financial and non-financial transactions.

Traditional banking is where clients directly visit the branch to do financial transactions, like deposits, withdrawals, or bank transfers. Because of the emergence of Internet banking, customers can do simple financial transactions faster and hassle-free through the help of Internet or mobile data, which they can process anywhere and anytime based on their preference. Internet banking conveniently provides faster and effortless banking transactions. According to the digital banking report of Finder.com issued last 2021 October, about 18% of Chinese adults, primarily men, have a digital bank account, which equates to an estimated 13,183,816 people. An increase of 18 % over the next five years is expected to double the digit by 2026. Moreover, with the latest trend in digital banking, financial institutions should highlight more transparency and be open to the acceptance of digitization rather than focusing only on traditional banking services. Concerning this COVID-19 surge paved the way for a more digitalized method of engaging the market; because of the restrictions of the pandemic, enhanced community quarantine and social distancing protocols created a need to have contactless transactions, especially in the Banking industry.

Although China showed faster progress in adopting Internet banking, the country is currently a cybercrime hotspot, underscoring the need to increase awareness and vigilance against the increasing prevalence of cybercrime in the country. (Wick Velasco, 2020). With this regard, cyberattacks have been a significant barrier to fully immersing Chinese bank depositors in interbanking facilities. With this in mind, Continuous research and enhancement of security measures will further help the gap and reach the untapped Internet banking market in China.

This study aims to understand the security measure of digital banking and how it affects the acceptance of online banking usage. Additionally, the effect of initial trust on Internet banking usage in China will be measured. Trust affects the commitment and loyalty that Internet banking can entice significantly (Lopez & Miguens & Vazquez, 2017). The research implies and examines whether these adoption factors influence higher confidence in adopting Internet banking despite financial transaction-related cyberattacks encountered. A sample of 350 respondents, Internet banking users, will participate in strengthening the data that will be presented.

1.1 Background of the Study

Compared to other Asian emerging market economies, Chinahas a relatively minor financial system that banks control. The system's total assets are equivalent to 126 percent of the GDP. Bank credit, however, accounts for slightly over 50% of GDP and primarily funds nonfinancial corporations (NFCs). Through conglomerate ownership, banks and NFCs are also closely related. Only a third of persons have formal accounts, which is a much lower percentage than in comparison systems for individual access to finance. Compared to banks, non-bank financial institutions and capital markets, particularly bond markets, are far less established. Fintech's ecosystem is still developing. (IMF Publications, 2022) The banking sector accounts for a significant share of the Chinese economy.

It is also regarded as the backbone of the economy, serving as a vital financial intermediary between the sectors of the economy. As a result, the development and comprehensive statistical data are essential to the economy's overall health. It implies a modification in terms of trends, lifestyle, industries, and strategies in line with the movement of the economy yearly. Banks increasingly use the Internet to get inputs and supply their clients with goods and services.

The Internet's popularity has overgrown, and it is now widely recognized as the ideal platform for distributing products and services. Thus, the use of Internet banking reduces cost and boost the speed of service.

The central bank is anticipating that digital financial institutions will support the Central Bank of China in reaching its goal of converting 50% of overall retail transactions from traditional banking in China to digital and increasing the number of Chinese adults with bank accounts to 70% by 2023. (China News Agency, 2022). In this regard, the Central Bank of China strongly supports the Chinese Identification system, allowing unbanked Chinese to open an account without going to the physical branch, accelerating financial inclusion. The Financial Consumer Protection Act would improve customer safety and trust in the digital bank system by strengthening the Central Bank of China's authority to address consumer concerns about digital financial accounts and transactions. (Benjamin Diokno, 2022)

China Banking Corporation (China Bank) is one of China's leading private universal banks. Through subsidiaries, China Bank Savings, China Bank Capital, China Bank Securities, China Bank Insurance Brokers, and Manulife China Bank Life Assurance, Chinabank provides a full range of banking products and services to institutional (corporate, middle market/commercial, SMEs) and individual (retail, mass affluent, high net worth) clients, as well as thrift banking, investment banking, insurance brokerage, and bancassurance. China Bank was founded in 1920 as one of the first privately-owned local commercial banks and thoroughly understands how entrepreneurs and businessmen conduct themselves.

Chinabank expanded the scope of its products and services to cover all market segments while maintaining very close multi-generational connections with the Chinese-Filipino community.

The Bank of the Philippine Islands (BPI) is a universal bank that is the fourth largest in terms of investments, the second largest in market capitalization, and one of the most profitable banks in the Philippines. The BPI institution, formerly El Banco Español Filipino de Isabel II, marked the beginning of the Philippine banking and finance industry. The bank performed many functions, including lending to the National Treasury and printing and issuing currency, making it the country's first Central Bank. Today, BPI proudly continues this tradition by funding numerous private and public sector initiatives and enterprises that promote economic growth and nation-building. The bank has over 1,170 branches in the Philippines, Hong Kong, and Europe and over 3,000 ATMs and CDMs.

The company offers a wide range of retail and business banking bank products. BPI is made up of numerous networks of branches that serve the expanding microfinance - small and medium enterprise finance industry sector. Clients of BPI have access to both online and mobile banking. It is one of the most widely used financial apps among Filipinos.

Metropolitan Bank and Trust Company (Metrobank) is the Philippines' second- largest bank. George Ty established it. It provides a wide range of financial services, from traditional banking to insurance. It was founded in 1962 and quickly rose to become the premier universal bank among major financial institutions. Metrobank operates a global network of 957 local and international branches/offices, remittance offices, and subsidiaries. Investment banking, thrift banking, leasing and financing, bancassurance, and credit cards are among the products offered by the bank.

Banco De Oro (BDO or BDO Unibank Inc., founded on January 2, 1968, is a full-service universal bank that provides a comprehensive range of industry-leading bank products and services such as deposits, lending, foreign exchange, brokerage, trust and investments, retail banking, credit cards, leasing, remittances, and more. BDO's organizational capabilities and value-added goods and services are the foundation of its customer relationships. Its branches continue to be at the forefront of creating high standards as a customer-focused sales and service force. BDO's organizational capabilities and value-added goods and services are the foundation of its customer relationships. Its branches, on the front lines, continue to set high standards as a sales and service-oriented, customer-focused force.

With over 1,500 functioning branches and offices and over 4,400 ATMs nationally, the Bank has the greatest distribution network. BDO has 16 worldwide offices across Asia, Europe, North America, and the Middle East (including full-service branches in Hong Kong and Singapore).EastWest Bank, founded in 1994, is now one of the country's fastestgrowing banks. It serves the financial needs of individuals, small businesses, and the mass affluent. It offers a wide range of banking products and services, as well as linked financial services such as non-life insurance brokerage, bancassurance, and leasing, through its statewide network of outlets. EastWest is working to expand its asset base, optimize its store network, establish new revenue streams, and diversify its distribution methods. At the same time, the bank is working to improve its information technology, risk management, and operational processes, as well as its staff professional qualities, in order to better serve clients.

China encountered different online scams, cyberattacks, and Internet banking issues involving a large amount of money, so Chinese banking clients hesitate to adopt Internet banking. “Cybersecurity and technology-related incidents are not completely avoidable,” the Central Bank of China said. “This is due to the inherent vulnerabilities in systems, technologies, processes, and people, as well as the persistent risks from cyber threat actors.”

Additionally, According to Riddhi Dutta of the back base, the Philippines has a high internet usage with a large unbanked population, so banks should give Filipinos a simplified digital platform to digitally emerge them to internet banking.

1.2 Theoretical Framework

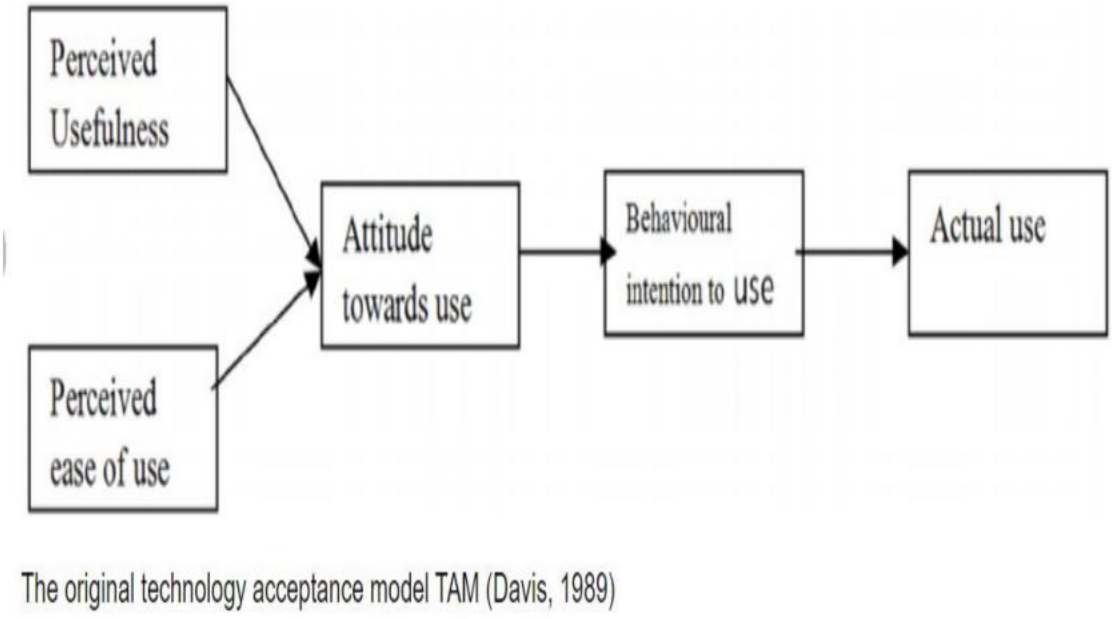

Figure 1. Technology Acceptance Model (TAM). Davis, Bagozzi & Warshaw,

The well-known Technology Acceptance methodology (TAM) is a methodology for articulating the benefits of online consumption. Perceived ease and Usefulness are two factors that impact how well a user embraces information technology, according to Davis (1989). Researchers frequently use this TAM to explain user behavior when implementing information technology. This investigation into the internet buying channel relies on the TAM's point of view.

Davis defines perceived Usefulness as "the extent to which a person believes that using a particular system would enhance his or her job performance." This determinant shows how people use or not use an application based on how helpful they find it for better performance, but more is needed to predict whether or not a user will accept the technology. (Karkar, A., Fatlawi, H., & Al-Jobouri, A. 2020)

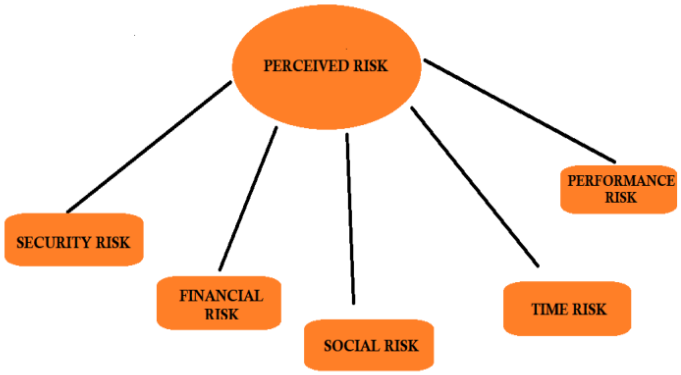

Figure 2. Theory of Perceived Risks (TPR)

Financial, performance, social, physical, security, and time risks are the six categories of perceived risk that have been determined (Jacoby & Kaplan, 1972; Kaplan et al., 1974; Roselius, 1971). A security risk is "a potential loss due to fraud or a hacker compromising the security of an online bank User" (Reavley, 2005). Financial risk is the possibility of financial loss due to transaction error or bank account misuse. (2007) Kuisma et al. Social risk is the likelihood that using digital banking may cause others in the family, circle of friends, or workplace to disapprove (Lee, 2009). Time risk can relate to the inconvenience and time spent due to receiving payment inefficiencies or troublesome navigation.

1.3. Conceptual Framework

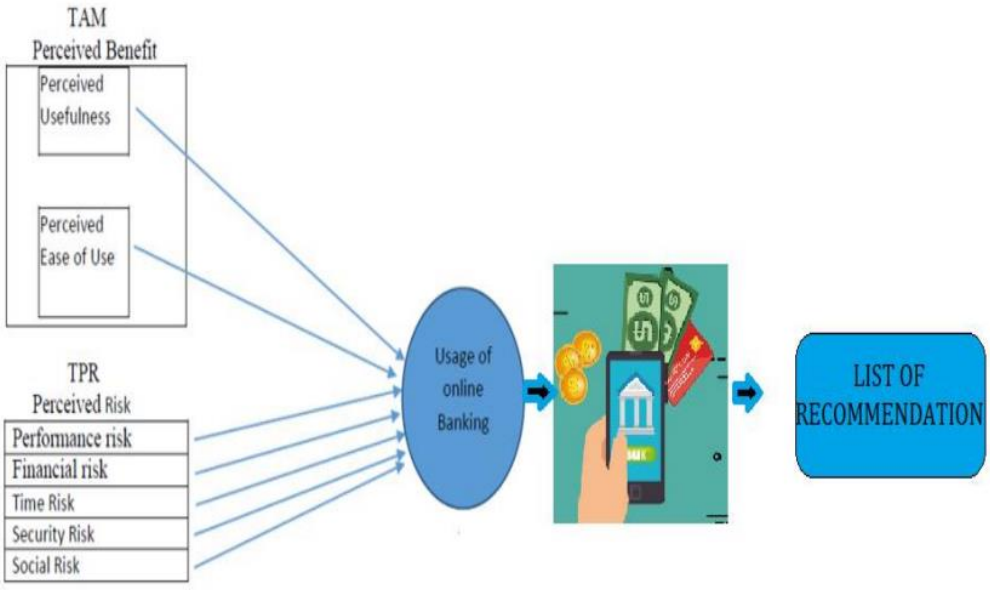

Figure 3. Research Paradigm

This paper suggests that perceived usefulness and ease of use directly influence users' attitudes and that the perceived risk can gauge the level of security measures and adoption of mobile banking in China. TAM theory and TPR theory framework worked to create a model for electronic banking that has not received any attention in earlier research and fills in the gap. The suggested framework includes five areas of perceived risk to offer an in-depth review that addresses both the advantages and disadvantages of online banking.

The findings support the proposed model's robustness in predicting customers' intentions to use such services and demonstrate its solid capacity for explanation (A. Sanayei & E. Bahman, 2012). Therefore, this study seeks to fill this gap by formulating research hypotheses based on an approach that integrates the theories used in the current study.

1.4 Statement of the Problem

The main objective of this study is to assess the security measures of digital banking as a basis for improving services. Specifically, the study aimed to answer the following questions given below:

1. What is the profile of respondents in terms of:

1.1. Ages;

1.2. Sex;

1.3. Source of income; and

1.4. Frequency of using digital banking?

2. How do the respondents' asses the security measures on digital banking as a basis for improving services in terms of:

2.1. Trust & Security;

2.2. Knowledge and Awareness;

2.3. Ease of Use and; and

2.4. Usefulness?

3. Is there a significant difference in the assessment of the respondents on the security measures of digital banking as a basis for improve services in terms of stated variables: Trust & security, Knowledge and awareness, Ease of usefulness and usefulness?

4. What common digital banking issues or problems encountered by the respondents?

5. What basis or inputs for improved services can be suggested based on the findings of the study?

1.4 Hypothesis

1. There is no significant difference in the respondents' perception of digital banking.

1.4.1 Scope and Limitations of the Study

This study focuses on the security measure of digital banking as a basis for improved services under the dimensions of Trust & Security, Knowledge and Awareness, Ease of Use, and Usefulness. The research will be composed of 360 respondents. The researcher uses a survey questionnaire to gather data through online forms to cater to additional respondents.

This study will be conducted in the 2nd quarter of the year 2023. The empirical results conveyed here should be considered in light of several limitations in terms of time constraints, availability of the respondents, and the locality of the respondents are mainly gathered within the different bank branches in China that will represent the population.

This study is composed of one (1) group of respondents, which are Customers or Clients of the bank who identify as the user of digital banking. One of the study's drawbacks is the limited amount of time available for data collection. The study was conducted academic year 2023.

1.4.2 Significance of the Study

The result of this study aimed to inform valuable data on how Internet banking adoption issues affect Chinese bank depositors. Moreover, this study will provide insight into how to improve the security measures of Internet banking in China, a secure alternative way to do their banking transactions. These findings will be essential to the following:

Bank Employees. The study will help bank employees to have a basis for understanding the hesitations of clients in adopting internet banking. Thus, Bank employees will be more aware and informed on how to explain the measures to secure the usage of internet banking despite the adoption issues in internet banking.

Banking Institutions. The study will help the Banking institutions evaluate its adoption issues and why clients hesitate to use internet banking. Concerning this, it will enable banking institutions to enhance their system and transcend in a more secure and reliable Internet banking experience for their clients.

Customers. The study will help customers to gain trust and confidence in using internet banking by being more aware and knowledgeable about the use of digital banking. It will also contribute to the level of perceived usefulness and improve customer satisfaction.

Researcher. The study is important to the researcher I partial fulfillment of thesis requirements to qualify for a degree in Doctor in Business administration.

Future Researcher. The study will serve as a point of reference for future researchers. This study can be a great help of substance and update research in similar fields of study.

1.5 Definition of Terms

The following terms were operationally defined for a better and easier understanding of the study*;*

Age. In this study, it refers to the age profile of respondents as a basis of their reliability in providing data for the study.
Digital Banking. This study refers to digitizing all of the banking operations and substituting the bank's physical presence with an everlasting online presence, eliminating a consumer's need to visit a branch.
Digital Banking Issues or Problems. In this study, it refers to the operational challenges experienced by banks, clients and other stakeholders in utilizing digital banking.
Ease of Use. In this study, it refers to the basic concept that describes how easily users can utilize digital banking.
Frequency of Using Digital Banking. This study refers to the client's and bank employee's frequency of utilizing digital banking services.
Improved Services. In this study, it refers to the output of the study that can be proposed to banks with digital banking services.
Knowledge and Awareness. This study refers to the clients, and bank employee's knowledge and level of awareness of digital banking services.
Security Measures. This study refers to the measures taken as a precaution against theft or, espionage or sabotage in digital banking services.
Sex. In this study, it refers to the sex profile of the respondents as it may affect the data to be gathered for the study.
Source of Income. In this study it refers to the various sources of income of the respondents that may have a relationship to their frequency of utilizing digital banking.
Trust and Security. This study refers to the client's and bank employees' trust and assurance of security to the digital banking services.

2. Review of Related Literature

The following discussions lay out the various reviews of related literature and studies in a topic framework to better guide the researcher's approach to the investigation.

2.1 Banking Industry

The banking industry plays an essential role in the daily life of modern society worldwide. From its inception, innovation is not new to the global banking system, evolving from the utilization of coins, banknotes, ATMs, and the lending system. Likewise, technology and innovation in the banking sector have transformed from time to time (Scardovi, 2017). Disruptive innovation, digitalization, and new technology are transforming traditional business models and processes. As a result, banks should modify their business strategies to change how they interact with customers, handle middle and back-office operations, be competitive, and be prepared for the future (Kitsios & et al., 2021)

New banking and financial payment methods have emerged due to the widespread adoption of the internet and mobile devices worldwide. Digital banking was established as a cutting-edge, practical, and effective method of financial transactions. There are numerous types of digital banking available right now, including mobile wallets, online banking, internet banking, and electronic banking(Alkhowaiter, 2020). Typical functions include viewing balance inquiries, transferring funds, and payments. When the economic crisis rose caused by the global COVID-19 pandemic, digital banking became an enabler in facilitating business transactions. The digital ecosystem linked banks to entrepreneurs, suppliers, employees, and new markets. Governments attempt to promptly and effectively dispense assistance to those in need. Simultaneously, digital banking allows for social distancing and helps foster financial inclusion in remote or impoverished places where financial institutions are not physically present.

2.2 Digitalization in Banking Industry

The automation of core banking services is known as digital banking or e-banking services. The change in banking services makes it possible for bank customers to use online or electronic platforms to access banking products and do financial transactions at their own pace. The digitalization of all banking activities has replaced the physical presence of the bank and removed the requirement for customers to visit the branch. (Harralaya, 2021). The banks are adopting online services for their transactions to stay competitive and bring positive customer service without the customer going to the branch. (Ahmed et al., 2020) There is a need to satisfy online customers in a competitive environment. According to the OECD (2020), they quoted that "Banking will move to a customer-centric platform," meaning the customer in the focal point of any business-related activities such as products and services. The digital disruption of banking increases competence and ability to provide service to clients and the gaps bridged by the present study.

Offering a user-friendly client interface helps to overcome the information gap. The primary threat to existing financial institutions is that influential technological companies will attempt to control the consumer interface through the use of superior data, acting as gatekeepers to the distribution of financial products. If this occurs, incumbent banks will be reduced to product providers on platforms over which they have no control; their businesses will be standardized.

The banking system is one of the major aspects driving the economy of a country. A variety of banking systems and operations has been the synergy that classifies the modern banking system. The bank houses one of the valuables, the "almighty money", the force that drives both the good and the bad conceptual ideologies of the world today. The might of money and what money can do has made its desire and demand second-to-none. Money is a deity that rules the world. Today, no money invariably means no nation, no man, so bad such that some people exchange integrity, even life, all to have money. Rubbers will bring down buildings, take away peoples' lives, do all forms of atrocities, all for money. Politicians can run down a whole system just to embezzle public funds for personal sake. The worst is in developing countries where the slogan for livelihood is "survival of the fittest", which implies the elimination of the unfit. The quest for money by all classes of citizens has made money an essential commodity such that the legal means to acquire money has been bastardized. Today, you can rub, murder, steal, burgle, kidnap or commit fraud to get money. Based on this, wherever money is housed, is endangered, who ever owns much money and is publicly known is also at risk of those who will want to forcefully own the money. Because of the numerous problems associated with the safe keeping of money, monies are kept in strong rooms with maximum security, convey in a security tide van with adequate and well-equipped security men, and the amount of money own, accessed, deposited, withdrawn or transfer at any point in time by individuals or corporative is being regulated by money laundry policy nationally and internationally. Statutorily, monies are kept in the bank for safe keeping, though there are instances of breaking into banks and carting away huge sums of money. This would have been worst if monies were kept by individuals at homes in large sums. The convenience of managing bank customers satisfactorily necessitated the introduction of electronic banking such as internet banking, mobile banking, SMS banking, phone banking, etc., where the banking system is 24 hours a day, 7 days a week, 4 weeks a month, and 12 months in the year at the customers convenient and disposal, provided he or she has the gadgets to effect same. Electronic banking has been integrated with evolving securities in accordance with evolution in knowledge and technology, but still, fraudsters take advantage of the social engineering vulnerability and the lack of trust and integrity of the bankers to defraud banks and bank customers through the electronic banking platform. For instance, the USA lost about $3.5 trillion daily through three payment networks, which dwarf the bank of New York. In February 2005, a Miami businessman sues his bank for the loss of $90,000, which was stolen from his online banking account by an unauthorized transaction. On investigation of the matter, it was discovered that the transaction was affected by his computer, which was infected with a Trojan capable of logging keystrokes invading his full account details. According to Ahmed et al. (2017), the prevalence of malicious applications that steal financial account information has measured dramatically over the years, which often result in victims losing a huge amount of money. Electronic banking fraud gain momentum in the early years, probably due to the higher chances of succeed than expected. At these times, Trojan was the prevalent avenue used in stealing financial account information, targeted only at a handful of online banks. Wǔeest (2020) analyzed the Trojan used in stealing the financial details of individuals as follows: PWSteal: it is a Trojan that was discovered in April 2005 that stole account information from five banks. It contained a list of 2,764 URLs from 59 different domains.

Trojan.Goldun: this was another Trojan discovered in April 2005 which steals an account from an online payment service called e-gold. Goldum (2020) disguised itself as a security update for the e-gold organization. It presents a deceptive file named security e-gold.exe. Once a user executes the deceptive file, the Trojan will register itself as a Browser Helper Object (BHO), where it monitors for visits to the predefined URLs from which it gathers the account information of victims. The account information gathered was transmitted through a PHP script to a domain mounted by the attacker. It has become imperative for banks which offer online banking to integrate efficient security models. In the past years, the growth of malware and exploits targeting online

banking vulnerability has been growing steadily. In 2009, it was reported that the 50 main electronic threats were bank Trojans. In an attempt to provide more secured security to electronic banking was the introduction of several security techniques such as the use of PIN, digital certificates, virtual keyboards, Browser protection, etc. (Smith, 2019). Data validation technique was proposed in 2014 by Aljawarneh and co. in their work title Usage of data validation techniques in online banking: A perspective and case study. The essence of the work was to consider the integrity of data (i.e. authentication of the source of data) to ensure that it is from a reliable source before it is given access to be used in electronic banking platforms (Rendell, 2022). Proposed also was the use of biometric security to ensure that the user of an electronic banking application is the only one who can access his account using biometric authentication (Smith, 2019). Salihu (2019) suggested the inclusion of Geographical Position Locations (GPs) with real time security systems to unveil criminals' anonymity. This paper takes a critical examination of electronic banking system techniques.

Attacks on Electronic Banking Systems Attacks on electronic banking systems simply referred to measures or techniques used in breaking into electronic banking transactions fraudulently. Subsoru (2022) analyses online electronic banking attacks to include Social Engineering: attacks based on tricking customers into divulging their secret identities to fraudsters through social media. The fraudsters make use of customers' limited knowledge of computer systems to their fraudulent advantage. They send text messages, calls, or links (phishing and spooling) to customers demanding their secret banking information, through which they take advantage of their victims and defraud them. Port Scanners: Attackers use various techniques to steal customers' information by using port scanners to ascertain entry points of customers into a system. Here, they place software which do repeated scanning of the information going through the targeted port until they are able to sniff customer's banking information. Packet Sniffers: Attackers mount surveillance on the connection between the user's computer and the web server to sniff customers' information, including credit card information and password. It, therefore, becomes possible to defraud such victims. Password Cracking: This involves the use of Brute Force and other vulnerability decrypting techniques to crack customers' user names and passwords for a specific website by scanning thousands of common terms, words, activities and names until a combination of them is granted access to a server; Trojans: A Trojan is a software that masquerade a host system requesting for a gateway before access is granted. Trojan is said to be the most dangerous security threat to electronic transactions due to its ability to secretly connect and send confidential information about customers secret information. Trojans are developed with the intention of anonymity. They can be used to filter data from many different clients, servers and database systems. They can be installed as surveillance on emails, internet messages, database communications, and other services. Denial of Service Attacks: The attack is used to overload servers and render them vulnerable. The technique is to place a heavy chunk of tasks on the server repeatedly until the server could no longer function well. The attacker then uses the vulnerability of the server at the moment and install a virus or Trojan onto the users' PCs and instruct them to carry out a specific attack on the server. vii. Server Bugs: Server bugs are used to confuse the server intrusion detection system, thereby allowing attackers the opportunity to generate threads with millions of web servers in use around the world. This renders the server vulnerable to the onslaught of server bugs and threats. Super User Exploits: This is a technique which allows the attackers to gain control of the system as if they were the system administrator. This is achieved by the use of scripts by the attackers to manipulate the database or buffer overflow that cripples the system. 1.2. Electronic Banking Security Techniques The advances in technology, such as the super-fast broadcast broadband connections for real time transmission, the high definition of 3D and 4D video content to personal homes, the emergence of cloud computing, the complemented physical network infrastructure such as WiFi, 3G, 4G, Wimax, etc., has enhanced and encouraged the application of technology in information processing and online businesses [xi]. On the same technology, electronic banking finds its operation. For the sensitive nature of electronic banking, the following security measures have been put in place as stated by [xiv] and [xii]), [x]. I. Digital Certificate: Digital certificate requires a trusted third-party who ascertains the authenticity of the transaction by signing the authentication certificates attesting their validity. The authentication depends on public key transaction (PKI) and certificate authority (CA). A digital certificate is used to authenticate both the user and the bank. II. One Time Password Tokens: A one-time password token is a second authentication factor, which is a code in the form of a password requested in a specific or random situation generated by the application and forwarded to a registered device of the user. The operation is authenticated and preceded if the password is entered as required within the predefined time interval. This measure renders captured authentication data by fraudsters useless for future attacks; hence, the password is changed dynamically and used once within the allowable time frame. III. One-Time Password Cards: A one-Time password card is a card used in generating passwords which are used for a second authentication factor like the One-Time Password Tokens. The challenge with One-Time password cards is that some banks allow for the reuse of passwords generated over some time, which makes them vulnerable to attacks. IV. Browser Protection: Browser protection is a security model which is secured at the internet browser level used to access the banking system. In browser protection, the user and its browser are secured against known malware. This is achieved by monitoring the memory area allocated by the browser with the intention of detecting such malware, as well as hindering credential theft and capturing of sensitive

information. V. Virtual Keyboard: Virtual keyboard in recent times has been replaced with a more efficient method that requires less processing power and slower transmission rate. A virtual keyboard is a device usually based on Java and software cryptography, which allows portability between different devices. Virtual keyboards thwart the efficient use of key loggers, which capture information typed into the device. VI. Device Registering: in the case of registering with the banking system for an online transaction, the device to be used by the customer is registered with the bank database (especially in mobile banking). The bank will, in the cause of the transaction, ensures that the registered device is the one used for such a transaction; otherwise, such transaction is refuted. For better authentication, hardware fingerprinting techniques are used in conjunction with user identification through secret credentials. VII. CAPTCHA: CAPTCHA solution is an automated test designed to detect and render ineffective automated attacks against authentic services. CAPTCHA solution helps to safe guard the customer from password guessing attacks on the identity. The method conveys information to the user in the form of scrambled images, which automated robots find difficulty to recognize and process. When the user is able to enter the scrambled image correctly, it makes him or her a legitimate user. VIII. Short Message Service (SMS). SMS is used to send short messages to a dedicated phone number of the owner of the account, seeking authorization to go ahead with such a transaction. IX. Device Identification: This technique is used together with the device registration. The method uses the physical characteristics of the user's device to identify the original and historical information of the users. X. Positive Identification: In positive identification, the user is expected to supply some secret information only known to him as a means of identity. This information must have been provided and saved in the banking database against the customer's session the first time using the banking application. XI. Pass-Phrase: Pass-phrase is likened to a password, except that it is a phrase. Pass-phrase is a second authentication factor which requires that a customer identifies himself by providing a phrase held by him as a gateway. XII. Transaction Monitoring: Transaction Monitoring requires the use of a business auditing model to monitor activity such as payment processing. The logs are monitored and reviewed to detect patterns of inappropriate transactions at the business process level. XIII. Education: As a basic requirement for electronic banking security defense, the user (customer) should have a very good knowledge of electronic banking security trends. By so doing, it becomes pertinent for the customer to provide strong passwords and avoid all forms of internet practices which are security vulnerable. XIV. Personal Firewalls: This is concerned with the use of firewalls to limit the types of traffic initiated and directed to your computer. XV. Secure Sockets Layer (SSL): The SSL model is a protocol that encrypts data between the customer's system and the site's server. The SSL monitors requests made from an SSL protected page by; Identifying the server as a trusted entity Initiate a handshake to pass encrypted information back and forth between the customer's system and the site's server. The idea is to ensure that information passing back and forth between the customer's system and the site's server is encrypted to make it meaningless, incase hackers intercept and sniff the information. XVI. Server Firewalls: A firewall houses the web server to ensure that all requests made enter the system from specialized ports only and, in some cases, ensure that all access is from certain physical machines only. Demilitarized zone (DMZ) using two (2) firewalls is the common technique use in server firewall security, which are (a) The outer firewalls that monitor the ingoing and outgoing HTTP requests while the client browser communicates with the server. (b) The inner firewalls which sit behind the e-commerce server. The two firewalls are built with intrusion detection software, which is used to detect any unauthorized access attempt. The server firewalls also used the honey pot server technique in addition to the DMZ. The honey pot is a resource such as a fake payment server, which is placed in the DMZ to deceive the hackers into thinking that he or she has gained access to the system. Surveillance is placed on the servers and closely monitored to detect access by an attacker. XVII. Intrusion Detection and Audit of security Log: A good security system is one that can detect and prevent attacks. The intrusion detection system monitors the activities of the users of the system and uses intelligent build-in- software to detect suspicious activities either based on role functions or attempts to access resources out of sites. The intrusion detection system, on detecting abnormality in the operations of the user, will block the user or log him or her out, then generate messages to the system Admin for thorough investigation and apprehension where possible. [3], proposed data validation techniques as a measure of online banking security. In their work, they observed that the main security issue in electronic banking was the absent or insufficient data validation technique. Security issues of electronic banking caused by input validation include i. Parameter manipulation leads to the subversion of logic or security control. ii. Code injection, such as cross site scripting, Structural Query Language (SQL) injection and operating system command injection attacks. iii. Legacy CLC++ vulnerability classes, such as buffer overflows, integer wrap and format string vulnerabilities [iii]. [xiii] defines data validation as the process of ensuring that a web application operates on clean, correct and meaningful data. This implies that a data validation rule should be applied to online banking systems to check for correctness, meaningfulness and security of data. In support of all the proposed and implemented security measures for electronic banking, [xi] observed that biometrics is an ideal tool for a person's authentication for applications on online transactions. They defined biometrics as measurable physiological and behavioural characteristics such as fingerprints, iris, face, voice and handwritten signatures. Biometrics requires the physical presence of the person; as such, it cannot be easily guessed, forged or lost. With these features of biometrics, it, therefore, becomes a very outstanding measure for online authentication. 2.

Safety Measures Required by Customers as a Defence against Electronic Banking Fraud [vii], [vi], [i], stated the following as safe practices by bank customers against electronic banking fraud;

1) End users should adopt good online habits and necessary precautions against being circumvented.
2) Customers should keep their account details as top secrets
3) Customers should be conscious of social engineering tactics.
4) Customers should be acquainted with bank security measures such as; - Confirm that the URL of the website is the same as that of their bank. - Ensure that the SSL certificate of the website issued to his bank is by a trusted certifying agent and within the validity period. - Ensure that the website process is the same when accessed from a different device.
5) Customers should practice safe surfing habits.
6) Customers should check their bank account transactions regularly for variations.
7) Update your device regularly with antivirus software, operating system patches, firewalls, etc, and ensure that your browser is set to the highest level of security.
8) Be careful of unsolicited emails or phone calls requesting PINs or passwords. 9) Always type your bank address into your web browser.
9) Never enter your personal details in a link you follow in an email
10) Ensure that before you do your online banking transactions, there is either a locked padlock or an unbroken key symbol in your browser window.
11) Ensure that you double check the account number you want to use for making payments before effecting such payments.
13) Never leave your computer idle when you are already login

14) Always logout when you are done with your online transactions.

15) Be careful of unexpected or suspicious popup windows that appear during your online banking session.

Electronic banking holds much deliverables in today's banking transactions and the future. The banking system has been miniaturized such that, as portable as the mobile phone is, it can carry the whole banking system, making banking services available to customers any-where-you-go. This is achieved by simply connecting the user's website from his portable and mobile device (i.e. from the end user) to his site in the bank server. The transaction requires a to-and-fro communication between the client's server and the host. Attackers make use of the communication gab and system vulnerabilities, such as parameter manipulation, code injection, legacy C/C++ vulnerability classes, etc, to hack into customers' information, which they equally use to defraud their victim [iii]. The security issue is a great concern of the modern electronic banking system. Several measures have been put in place by banks hosting electronic banking to combat the ugly trends, but total control of electronic banking fraud is yet to be achieved. In the event of finding a lasting solution to electronic banking fraud, [iii] proposed data validation techniques for online banking. [xi] proposed the use of biometrics authentication for electronic banking. Biometric authentication, in combination with other techniques, holds the promise of providing authentic security for online banking, but the application of biometric in real time application, especially in a growing database like those of banks, is challenged by the weight and graphic nature of biometrics, hence, it requires a larger storage capability, and a very high, speed CPU [xiii]. In addition to the security system in placed or proposed, [ii] is of the view that a model that will unveil fraudster anonymity and a special court dedicated to quick prosecution of fraudsters should be put in place to serve as a deterrent to prospective fraudsters. Also, there is a need for users' awareness of security threats and practices vulnerable to electronic banking security. It is the expectation of the researchers that if these security measures are put in place for electronic banking, then the issues of electronic banking fraud would have been a history

2.3 E-Service Quality and Internet Banking

As the channels of service delivery shifted from traditional to electronic, the need for a scale to measure the e-service quality was felt. Researchers have developed many scales to evaluate Web sites. A rating scale for websites called WebQual was created by Lociacono et al. This scale was based on twelve dimensions, namely informational fit to task, interaction, trust, response time, design, intuitiveness, visual appeal, innovativeness, flow, emotional appeal, integrated communication, business processes, and substitutability. Convenience, accuracy, efficiency, queue management, accessibility, and customization, as well as feedback and complaint management. The link between online services and customer satisfaction in Internet banking and discovered a substantial link between the online service quality dimensions of fulfillment and efficiency and customer satisfaction with electronic service quality. personalization, technology updates and logistic/technical equipment.

Mobile banking is a type of electronic banking or online banking in which financial services are provided via a mobile device. Mobile banking (m-banking) refers to online transactions carried out using mobile devices and wireless telecommunication

networks. Mobile banking is defined as a banking channel that allows banks and their customers to interact via applications or browsers on mobile devices. It refers to financial transactions that can be carried out using mobile communication technology. In contrast to online banking, mobile banking requires at least one part of the banking transaction to be completed using a mobile device. Brundel C., & Azrioua S. (May 2018)

2.4 Security Measures on Digital Banking

Trust & Security

In the issue of trust and security in the utilization of digital banking, Vejačk (2021) found out that security measures ply an important role in winning the trust of individuals. The dynamical development of information and communication technologies has been one of the major factors of economic growth. Electronic commerce allowed the selling and buying of products or services to many times larger number of customers than ever before. Electronic banking, as a part of electronic commerce, is nowadays a very important distribution channel for banking services. With the intense development of information and communication technologies also, several forms of electronic banking arose and also vanished.

Especially mobile banking has recorded turbulent development in recent decades. Mobile banking in smart devices, together with internet banking, are now the main forms asserting in the electronic banking market.

Competition among banks in the field of electronic banking pushes them to improve their electronic banking services to sustain or increase their market share. The important issue is the trust of bank customers in the form of electronic banking used. Banks' customers also sensitively perceive the security of electronic banking forms used by them. In this article, we mainly investigated the influence of security and trust on electronic banking adoption. A research model based on the technology acceptance model was developed, and research hypotheses based on this research model were constructed. The influence of perceived security, trust, attitude toward using and behavioral intention to use electronic banking in Slovakia was examined using factor analysis. The results reveal that all factors investigated have statistically significant direct and indirect effects on electronic banking adoption by users in the Slovak retail banking market.

Similarly, PYMNTS' (2023) latest research finds that despite a general satisfaction with existing security measures financial institutions (FIs) use, half of all adult consumers feel their banks must take additional steps to protect their assets and personal information, especially for non-routine transactions. Banks tend to meet basic online security expectations but fail to deliver the security options and features their customers prefer.

The study reveals that nearly three times as many consumers now prefer to access their bank accounts using smartphones rather than computers, with security playing a pivotal role in this shift. While most consumers now view smartphones and computers as equally secure, many see biometric authentication measures, which smartphones tend to provide, as the most secure way to authenticate a transaction. Moreover, the key findings from the report include the following: most consumers now believe smartphones and computers are equally secure for online financial activities; consumers view biometric tools as more secure than passwords for authenticating their transactions; and most consumers are satisfied with their banks' digital security measures, but half still believe that their FIs should do more.

In support of the claims of the reviewed studies on security and trust to the security measures of digital baking, Gabriel (2023) presented the influence of privacy of digital banking on the trust of the users. According to him, the growth and development of technology in recent times and the increased use of digital platforms by companies have set a new course in the work and personal lives of workers and users. This digital shift has revolutionized consumer behavior and commercial exchanges, where e-commerce is positioned at its peak. Moreover, in the banking sector, it is worth nothing how commercial banks and financial institutions have been implementing Internet e-banking services in the last decade.

However, digital banking does not involve direct contact with the individual; therefore, e-banks must offer a higher quality of service in order to compete. Banking customers' aspirations and interests in relation to service are expanding as technology progresses and evolves. In this regard, security and speed of transactions, ease of use, trust, and privacy issues are some of the main factors that customers consider when choosing a bank.

Moreover, Rendell (2022), in his article made, emphasis giving priority to the digital trust for the bank, particular during the post pandemic period, since the pandemic accelerated the shift to digital banking, and there's no going back.

Today's banks may never meet a customer in person. To minimize risk and keep customers secure, banks need to focus on building relationships based on strong digital trust. Under the principle of digital trust, a financial institution is highly confident that a digital banking customer is the person they claim to be and the person is authorized to perform the transaction they request. It's like a digital handshake between a bank and a customer where both parties transact together with confidence. But digital trust is a two-way street. With fraud increasing and fraudsters become more inventive, bank customers want assurance that their bank can keep them secure. If something about their account behavior seems suspicious, customers expect their banks to catch it and take measures to keep them and their money safe.

In another chapter of the article, Rendell (2022) presented the three important reasons why banks must increase their focus on developing digital trust. Fraudsters are targeting the end consumer. Banks have invested in fraud detection solutions that have made it harder for criminals to commit fraud. As a result, fraudsters are focusing their attention on the next most vulnerable cog in the transaction: the end consumer. Fraudsters might prey upon potential victims during a moment of weakness like a medical situation or by taking advantage of world events like the pandemic to push a scam. Secondly, banks can't intervene in customer transactions too often. Digital trust is essential for banks to allow customers to transact without a significant level of intervention. If the bank can't trust the customer is who they claim to be or that they are authorized to perform a transaction, the bank will have to take measures to authenticate the customer at multiple steps of their journey. Too much intervention leaves customers feeling irritated and annoyed at their bank. Finally, bank customers expect to be trusted.

Customers believe that their banks should know who they are based on their provided data. In their opinion, their bank should know that if their home address is in London, but they are suddenly making a high-value transaction in Brazil, something may be suspicious. If, however, they're carrying on with their daily routines and have to authenticate themselves repeatedly, they'll think their bank doesn't trust them.

On the other hand, Moscato et al. (2022) presented their finding on the perception of online banking security concerns. Accordingly, the concern about security is and always has been one of the major factors affecting the adoption of online banking. It is, therefore, essential for online banks to not only take proper security measures but to ensure that their customers and potential customers perceive their services as secure. This research highlights the significance of user perceptions of security by examining the content of the security policies of banks throughout the world. The security policy is illustrated as a tool for banks to use to manage their users' perceptions. The investigation also uncovers some notable differences among the expected security concerns within different regions. If banks understand their target audiences' e-commerce backgrounds, they can more effectively manage their potential users' perceptions of security.

Across the board, banks are found to be more vocal in their security policies about their transmission encryption than about their storage encryption. Transmission is the part of the transaction that the user experiences and takes part in. Storage happens behind the scenes in the purview of the bank and out of sight of the customer. Seemingly, banks would like to draw users' attention to the things that they can actually see during the transaction, bolstering the perception that security exists. This seems to be the main goal in portraying an online bank's security policy.

This finding is consistent with previous research that has indicated that Web users are influenced more by the security measures that are apparent during the transactions (such as a lock icon in the browser) than by those that are not visible (such as a digital certificate)Similarly, Smith (2019) revealed in his article the vulnerabilities of the digital banking despite of the various security measures conducted by the bank and other financial institutions. He clarified to the public, particularly to the target consumers, that not all electronic baking transaction is enabled by the internet. The option of using USSD (Unstructured Supplementary Service Data) or quick codes still abound. However, internet-enabled electronic banking transactions are far more prevalent. This service is provided by the bank as a means of streamlining its services to customers, thus reducing the banking hall population at any given time.

Most E-banking systems come with a user-friendly interface that, with proper guidance, even the least tech-savvy individuals can carry out transactions easily. However, the system is burdened with a major challenge, which is security. Security has been a primal concern with everything that pertains to being online, and the E-banking system is no exception. If malware fails to hit the system and disrupt the entire process, hackers would interfere and cause chaos in the system. These attacks could be a result of tiny security cracks on the website or on personal computers/gadgets.

User carelessness is another contributing factor. Mobile banking transaction loopholes further increase the security vulnerabilities of E-banking. Moreover, Smith (2019) presented in detail the online security vulnerabilities of electronic banking, which include

the following: first, Using Unsecured Wi-Fi Connections. Most customers will revel in the idea of free Wi-Fi connections to surf the web on the same PCs or mobiles with which they carry out electronic banking transactions. While the idea might seem cost effective, it could actually cost the user more when trouble sets in. Some of these Wi-Fi connections are unsecured and serve as the bait set by cyber criminals to gain access to the PCs or mobile systems of their targets. Using free Wi-Fi connections can lead to security and privacy breaches, one which cyber assailants stealthily hijack.

Secondly, the Third-Party Applications. This security challenge is more common in mobile banking. Usually, the banks instruct customers to download official apps from their website or recommend a trusted supplier to handle mobile application creation and control. However, customers usually prefer to download these apps themselves from mobile app stores, and this is a potential security breach that cybercriminals tend to exploit, always. Hackers could create an exact replica of the apps, stock them up with malware and put it out there for customers to download. These customers aren't software or app developers; they can't tell which is secure, so they download and run into problems.

Third is the Phishing Attacks. Internet fraudsters use a process called phishing to obtain private information on their prey, one that comes in handy when they wish to commit cyber atrocities. The phishing process involves the distribution of email messages or links that look legitimate to recipients. A click on such emails or links, which might require you to part with private info, is all that is needed to attack a victim's finances. Since most customers usually can't tell which email is from a trusted source or not, they are advised to apply discretion before clicking or open any link sent to them. If you do not feel sure about a link or email, it is best to chuck it in the spam folder of your email and contact your financial institution.

Fourth, the Slip-ups and Omissions. This is an internal security challenge. In the course of data capturing, errors can be made either intentionally or not, either from the data supplier or the customer's end, which bypasses fraud/error detection systems. A wrongful supply of sensitive information used in creating a personal banking profile may leave loopholes for hackers to breach. Finally, the Staff Integrity. Internal staff who have access to the web database of the bank or the entire security framework could tamper with it and wreck the whole system. They could also water down the network's firewall, thus leaving it exposed to attackers.

This unprofessional behavior could stem from grievances against the management and are carried out as a form of a personal vendetta at the expense of the entire security of the financial institution and its clientele base.

In relation to the discussion of digital banking security measures, Amtual (2020) included the presentation of electronic banking security issues which may affect the trust and confidence of consumers to transact their business using digital banking. Accordingly, the providers of Internet banking services must be more responsive towards security requirements. While there is no doubt that Internet banking transactions should have layered protection against security threats, providers should approach security considerations as part of their service offerings. Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. Using biometrics for identification restrict individuals from access to physical spaces and electronic services. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

In addition to the electronic banking issue, Bansal (2020) gives emphasis on the effect of cyber security issues, which greatly affect online banking transactions. The cyber security concerns influencing online banking transactions are the subject of this investigation.

Cybercrimes are increasing as a result of the technology's rapid growth and widespread application in numerous industries. Online banking sectors, which include several firms, are dealing with cyber security and data breach challenges.

The study of numerous technologies and methodologies used in the creation of complicated software is aided by modern computer technology. In one step, modern computing techniques can tackle problems that are challenging for traditional computing methods. They offer a new method for performing calculations. Modern computing techniques are used to create specific types of computer security techniques. Modern computing systems employ a variety of cryptographic strategies to address cyber-related problems. The largest banking system, accepted by billions of users worldwide, is mobile banking. Due to their lack of understanding, some consumers are unsure whether to accept. These days, mobile banking is thriving in the majority of developing nations thanks to its low maintenance costs and convenient internet connectivity. Most consumers attempt to communicate with their money from any location in the world. The greatest way to satiate this demand is through M-Banking.

Customers can use the internet to access their bank accounts. It was also discovered that many customers occasionally need to sign in to their accounts from different devices. With so many devices logging in, hackers may be enticed to use the login history to log in. These days, mobile banking also has some positive societal consequences in the areas of governance, healthcare, agriculture, and education.

In Thailand, extensive internet banking security was experienced by the customers, as revealed in the findings of Subsorn (2022). Based on the outcome of the study, internet technology has influenced everyday life during the past few decades because of its capability to assist and enhance operational and managerial performance in both non-business and business industries.

Furthermore, security issues have become more common nowadays in internet technology, particularly in internet banking systems, due to the harmful impact on confidentiality, integrity and privacy of the bank and its customers. The findings from the research revealed that there were deficiencies in internet banking security in all selected Australian banks, which were likely to affect the confidentiality of the existing and potential customers of the banks. The aim of this paper was to further the scope of the research by investigating internet banking security in another country. It examined Thai commercial banks and compared the results/findings obtained from the previous research paper to generate a feasible guideline for Thai commercial banks. The investigation revealed that there was a distinct lack of internet banking security information provided on all the selected Thai banks' websites as compared to the selected Australian banks, which provided better internet banking security information.

2.5 Knowledge and Awareness

Internet banking security information is very important to build the trust and confidence of consumers in the utilization of digital banking. In the article of Shanmugapriya (2021) on customer awareness of digital banking, it is found that the majority of the customers are fully aware of digital banking; however, they have limited knowledge and capacity for the proper utilization of the system.

Accordingly, for the economic development of a country, the bank plays an important role. In fact, banking is the lifeblood of modern commerce. They have now come out to satisfy economic obligations in addition to their competitive business-oriented activities. The current level of economic growth and economic reforms has made the banking industry very competitive by offering customers different products and services. As the level of awareness increases, it leads to an increase in customer preference. Banks provide for the needs of agriculturists, industrialists, traders and all the other sections of the society.

Then, they really, thereby, continue to accelerate a country's economic growth. Similarly, Kiran (2022) presented the results of his findings on customer awareness and their preference for the utilization of digital banking.

The changing habits of consumers and the new competitive environment are forcing technology to change on a daily basis so as to survive in the market with a reasonable profit. The banking sector has also become a part of the race by addressing the digitalization process as a matter of urgency.

This sector also does not want to be left behind in a market where it finds itself in the full forms of transformation. Banks are not known to be fast movers in general. But with the ever-growing competition within the industry, they, especially the private sector banks, had initiated the facilities of digital banking.

The various banks are responding to this digital challenge by using different approaches and at varying speeds, but all companies don't understand what it means to transform into a digital bank in the same way. They have introduced various innovative methods of doing banking with a click and make it hassle-free.

Now, there is no need to visit the bank branch for petty information like knowing the account balance or to seek advice for investment. Phone banking, net banking and mobile banking are all made available by different banks for easier access.

In addition, the ATMs have also been installed in distant areas where, previously, the banking facilities were hardly found. Plus, the initiation of smart cards like debit cards or credit cards, making recharge and bill payments effortlessly while sitting in the comfort of home and some better offers and discounts are made available to customers as a part of such digital banking facilities. The public sector banks have been in a very stagnant position with a low turnover. But now, they have also started to follow the lead of private sector banks in adopting the digital banking system in the Indian financial market.

From net banking to e-wallets, all of these have been introduced and are being embraced by the public at large. Therefore, a study has been carried out to check the awareness and preferences of customers for digital products offered by HDFC bank. The most

commonly used digital products of the HDFC bank are net banking, mobile banking, debit cards and credit cards. However, people are not very aware of other innovative products like smart buy, payz app, chillr and POS machine. So, the bank should market their products aggressively and induce the customers to buy their products by providing certain offers and incentives. Marketing of these products should be done through virtual media, especially television media, so as to pitch maximum audience.

In the study made by Anene (2021), the level of awareness, acceptance, usage of the digital was given an emphasis in order to identify the impact of awareness on the utilization of digital banking. The study found that the majority of academic librarians are aware of and mostly used mobile banking services such as buying airtime (self), transfer money, check account balances, get account statements, buy airtime for others, make transaction enquiries, and SMS alerts.

Almost all the academic librarians agree and strongly agree that the adoption of mobile banking services hasten funds transfer, makes enquiries on account faster, saves time of the customers, enhance prompt response, more convenient to customers, and saves cost.

Network failure during transactions, chances of fraud, lack of information privacy, concerns related to non-delivery of transactions, system security is not guaranteed in case of loss of phone where identified as the challenges associated with the use of mobile banking services in Nigeria. Moreover, the adoption and use of mobile banking services will save the time of the customer by conducting their transactions quickly without having to queue up and to use paper documents. The study reported the present level of awareness, acceptance and use of mobile banking services by academic librarians who are customers of various banks in Nigeria. Arising from the analysis, the study found that the majority of academic librarians are aware of and mostly used mobile banking services such as buying airtime (self), transfer money, check account balance, get account statements, buy airtime for others, make transaction enquiry, and SMS alerts. Almost all the academic librarians agree and strongly agree that the adoption of mobile banking services hasten funds transfer, makes enquiries on account faster, saves time of the customers, enhance prompt response, more convenient to customers, and saves cost. Network failure during transactions, chances of fraud, lack of information privacy, concerns related to non-delivery of transactions, system security is not guaranteed in case of loss of phone was identified as the challenges associated with the use of mobile banking services in Nigeria.

The adoption of mobile banking services enables transactions to be done anywhere in the world and at the customer's convenience. As revealed in the study of Thomas (2021), the revolution in technology and evolution in awareness of internet banking has en-route to this descriptive research. The Study on awareness towards internet banking among senior citizens highlights as the Data are relays on respondents, i.e., senior citizens. Banks may extend customer meeting time with bank officials, and also friendly approach is necessary. It will automatically improve the banking service and development of banks. The study is useful to know consumer awareness of the internet banking system and what types of risks involved in the e-banking system and investigates the factors on hindrances, services rendered, supporting factors, etc.; the finding depicts that the customers use only limited facilities as per their awareness gained among the various availabilities of internet banking service available. Based on the findings, there is a lack of awareness about Internet Banking usage among rural people. Banks should take necessary steps to create awareness among them about the various services of Internet Banking that are available and also the advantages of using such services. Demonstration of Internet Banking should be provided to the customers to promote electronic banking. The banks should focus on the security issues regarding confidential credentials, which are at risk of hacking in the cyber world.

The cost involved in using Internet Banking services can be minimized in order to increase the number of users of Internet banking. The Internet Banking system should be enhanced to make online enquiry and online payment much easier for the customers. To increase efficiency, service quality of banks, safety, integrity, Internet Banking can be used in a rightful way.

Mohan (2022) in his report describes digital banking services. It aims to investigate factors influencing customers' impression of digital banking services, satisfaction and preference. The results show that people of all ages prefer digital banking to traditional. Customers use cell phones to complete digital banking.

These customers are pleased with digital banking services because they are convenient and widespread. These include the study's consequences, recommendations for improving digital banking services, and future research directions. Moreover, making people aware of the existence, functioning, and benefits of digital banking products and services is a huge work that has to be performed. Private financial institutions should host exhibits and talk programs for the public as well as offer goods and services that are available to everyone, regardless of their financial status. The bank could use more compelling advertising and awareness activities

to raise awareness. Spreading awareness of digital banking among people of various ages and socioeconomic backgrounds by teaching them about its advantages. Client confidence can only be earned by providing adequate transaction security.

Banks should make sure that no service cases are delayed due to a network fault if there are any. The bank's employees must be well-versed in all elements of digital banking in order to inform clients about these services sensibly. The bank could come up with additional commercials via bank flex in the branch to help customers understand how to use digital banking services when they visit any of their counter locations. Using the ATM more than three times will not result in extra charges. For the protection of customers and the security of transactions, government authorities should put up an appropriate regulatory framework. Always be cautious when using the internet from a public computer. Make your password difficult to guess. Education institutions must include practical knowledge in their curriculum if they want to teach students about Digital Banking as a specific topic.

According to Shaji (2020), the revolution in electronic technology has taken over the world. The banking sector has not been immune to the impact of this digital revolution. In India, both private and public banks have changed their standard business practices and have now shifted entirely to electronic banking. The banking transactions that are executed through electronic devices and over the internet are termed electronic banking. One of the special features of urbanization is that urbanized society, irrespective of gender, is ready to accept the change and adjust to the new technologies quickly because of their extensive exposure to these innovations and their higher educational standard.

This raises the question of how far these electronic banking reforms impact residents in rural areas, especially rural women who spend most of their lives within their homes. The present study has been undertaken to analyses the extent to which rural women are aware of electronic banking services with special reference to Nelamangala, which comes under the Bangalore Rural district of Karnataka state in India. The current research study is based on the usage of electronic banking services among rural women customers. It was an effort to examine the customers' awareness level and satisfaction level and also helped to check whether there is any difference in the satisfaction level of the customers.

As far as the awareness level is concerned, highly educated customers have more awareness, and awareness levels among the younger respondents are greater compared to older respondents. So effective measures need to take to enhance the awareness level of the customers of all age groups. In the present study, it is evident that rural women customers need more support and guidance to adapt fully to the electronic banking services offered by banks, as only 15% of the rural women respondents have a good understanding of the various e-banking services. In the study on awareness, utilization and barriers to the e-banking system, Kaur (2020) explain the primary purpose of the e-banking system. E-banking is electronic banking that provides financial services for individual clients by means of the Internet.

E-banking includes the systems that enable financial institution customers, individuals or businesses to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. A cross-sectional descriptive study was conducted with the aim of assessing the awareness level of utilization and explores barriers towards e banking among 200 bank customers in East Delhi, India, by using face-to-face interview techniques. Most were aware of the term ebanking, whereas 87.2% were about the services of e-banking. The majority have utilized e-banking services, and most of them have used them 4 times per month. The topmost used services were ATMs, online shopping, money transfers, credit cards and SMS banking. SBI is among the top choices of customers for using e-banking services. Most customers faced barriers to utilize e-banking services.

Satisfactory evidence was obtained regarding the utilization of e-banking services. ATM was the most popular as well as preferred e-banking transaction among the customers, followed by online shopping, money transfer, credit card, SMS banking, etc. SBI, ICICI and HDFC were the leading banks providing e-banking services to the clients. Most of the customers faced the problem of server down while using e-banking facilities. Awareness about the term e-banking and utilization of e banking were statistically significant with the age and educational status of respondents.

2.5 Ease of Use

The security measures of the digital banking system enable the customer to use it with easiness and it accessibility to all with its user friendly features. These is the findings in the study of Asif (2021) on internet banking usage between the elderly and youth. Findings indicate that there is a relationship between the experience of online banking and the experience of traditional banking.

The findings also reveal that there is enough evidence to support that there is a relationship between no. of years of usage and online banking. In this research, it is seen that internet banking is majorly used by the youth instead of visiting banks.

Whereas old people prefer visiting physically to banks as earlier in their time, there was no internet banking used that much as compared to this time. This research helps us to know the reason why the young generation prefer only internet banking and why the old people go to the bank physically and do not use internet banking. The youth should also visit the bank because it helps them to where the bank or their branch is situated and also gets to know who is their relationship manager and to whom they can complain about that branch if they will face any kind of problems. The youth can teach the elderly people how to use internet banking as at their age, the immunity of the body goes down as compared to the youths' immunity.

In the study conducted by Salihu (2019) on the effect of security and ease of use on reducing problems of electronic banking services, the use of technology in banking operations has facilitated many daily banking activities. However, the use of technology in electronic banking services has its problems/deficiencies as well. The study examines the impact of electronic banking services on security and ease of use. After a thorough review of the literature, this study provides a statistical analysis through a distributed questionnaire to examine the effect of security and ease of use in decreasing issues with electronic banking.

Regression analysis demonstrates that security and ease of use of electronic banking services have a negative effect on issues with electronic banking services, which implies that with enhanced security and/or ease of use, their issues are decreased.

Similar to the study of Titus (2021) on the customer perception of the ease of use of internet banking. Internet banking allows banks to provide information and offer services to their customers conveniently using internet technology.

However, studies have shown that customers have perceptions that impact the uptake and continuous usage of the platform. The purpose of this study is to understand the effect of customer perceptions on the usage of internet banking in commercial banks in Kenya. Based on the findings of the research, it was concluded that customers have perceptions that have an effect on the usage of internet banking.

These results indicate that complexity is an important element in understanding and using internet banking, which is indicative of whether customers adopt and continue using internet banking or not. Other researchers have empirically found a positive impact of bank web site design as a critical factor in the use of internet banking. Clear and simple help menus allow customers to perform internet banking transactions easily, and this increases customer satisfaction in the long run.

In Malaysia, the study by Ali (2020) revealed the consumers perceived ease of use and trust in online banking. According to him, the development and invention of technology has transformed the way organizations conduct their businesses currently, including banking institutions, mainly in offering online banking services. Online banking services have been introduced in Malaysia. Still, online banking users in Malaysia are intolerant of issues of trust towards online banking, which affects their level of acceptance. The findings showed that perceived ease of use and trust have a significant relationship with the intention to use internet banking. The outcomes offered valued information for both financiers and policy makers, particularly when designing online banking marketing approaches. In addition, the elements in the independent variables, namely perceived ease of use and trust were, become the utmost factors defining the acceptance of internet banking usage. Findings also discovered that there is a positive and strong relationship among the variables.

Among all variables, trust influenced most the intention to use the internet banking. Trust is a considerable component that contributed to online banking applications and the information technology team integrity that banks managed. Thus, the banking institutions should think through by emphasizing the benefits of using online banking to users, increase internet banking services to make it easy to use as well, as make up the security in the online banking transaction to improve the trust of consumers with the internet banking implementation.

2.6 Usefulness

The digital banking security measure increase the level of usefulness of online or digital banking aside from the level of knowledge and awareness, ease of use of the applications, and trust and confidence. The convenience provided by the digital banking enables the customers to transact their business remotely.

One of the key benefits or advantages of the utilization of digital banking, according to Rebello (2022), the digital banking can be described as the digitization or automation of almost all traditional banking activities and services, such as money transfers, making

payments, checking account balance and more with the use of secured digital channels. These banking activities and services were previously accessible only at the bank branch.

Digital banking has redefined banking for customers as it substitutes a bank's physical presence with its online presence, ensuring customers do not need to step out of their homes to take advantage of these services. With digital banking, customers can use digital wallets, online banking facilities, mobile appsfor payments and do much more. The rise of technology in the past 20 years has brought unprecedented changes to the world of banking. People can use the internet to perform various banking transactions with ease. Also, digital banking has resulted in a substantial increase in people adapting to online banking, and banks lowering transaction costs and improving operational efficiency through automation.

Moreover, the benefits of digital banking were discussed in the study, and these include the following: First, 24/7 Convenience. Digital banking offers customers 24/7 secure access to various banking services, eliminating the need to take a day off or plan their day to visit the bank branch during its working hours.

Digital banking apps help customers check their account balances, make payments, transfer money and do more from their mobile phones, wherever they are. Moreover, the boom in electronic banking has paved the way for cashless transactions, wherein people can pay for their purchases without having to carry wands of cash or having to visit a nearby ATM to withdraw cash. Cashless payments are secure, fast, convenient and allow customers to track the transactions electronically.

Secondly, the Multiple Features. Digital banking makes it easier to perform fund transfers locally and internationally. With digital banking, customers can also easily schedule payments for funds transfers and bill payments. Digital banking facilities help customers and banks go paperless as electronic statements can be securely shared to the customer's email. Furthermore, with a banking mobile app, customers can easily locate nearby ATMs make cardless ATM withdrawals, among others.

Third, Safety and Security. Enabling secured and safe online and mobile banking is one of the foremost precautions that banks need to take care of. Banks have added several safety features, such as the generation of a One-time Password (OTP) to complete a transaction. Also, digital transactions occur over secure servers and networks, ensuring better safety features than traditional money transfer options.

Finally, the Alerts and Notifications. Customers can opt-in to receive bank account alerts for transactions through emails, text messages or push notifications on their registered email/mobile number. This helps the customers to be aware of the transactions that are happening in their accounts.

3. Methodology

The research methodology covered the methodologies and procedures that were employed to conduct the investigation. This comprises the research design, population and sampling, study respondents and their demographics, research instrument, instrument validation, data collection technique, and statistical treatment used in data analysis.

3.1 Research Design

The researcher used a descriptive method of research and employed the use of a standard questionnaire. The descriptive research design involves gathering data that seeks to describe events and then organizing, tabulates, depicts, and describes the data collection in a systematic manner. (Glass, G. V., & Hopkins, K. D. 1984) The survey questionnaire is divided into two parts: the demographic profile of respondents and the list of questions that the researcher aims to know in order to collect valid and reliable data needed for the study. The second part was subdivided into 3 parts, which are Security Measures on Digital Banking, Common Digital Banking Issues and Problems Encountered by Respondents, and an open-ended question about Suggestions & other problems encountered.

3.2 Population and Sampling

The researcher employed the snowball sampling method or the chain referral sampling method. It is a sampling technique that includes a primary data source as well as the identification of additional potential data sources who will be able to participate in the study.

3.3 Respondents of the Study

The respondents of the study are composed of bank depositors who have an online banking account or had actual experience using any mobile banking application. The respondents who are considered clients are those respondents who have existing accounts or any bank products associated with the banks that are linked to the mobile banking application. The researcher target

sample is 350 respondents who are randomly selected and purposely selected based on the respondent's availability at the time of data collection.

3.4 Research Instrument and the Validation of the Instrument

This study made use of three hundred sixty (360) respondents. The survey questionnaire was used as the main gathering instrument for the acquisition of the needed data. Also, it includes the average weighted mean and T-Test as statistical tools. The study was conducted in Metro Manila using online applications such as google forms,

3.5 Data Gathering Procedure

The researcher employed the snowball sampling method or the chain referral sampling method. It is a sampling technique that includes a primary data source as well as the identification of additional potential data sources who will be able to participate in the study.

The distribution of the survey questionnaire started after the survey questionnaire was approved. Employee referral from different with the help of other colleagues will help the researcher to gather needed data faster. The researcher made use of an online form, which is a web-based tool that allows user to create fillable and customizable forms that can be shared with people on many platforms after it has been made. The user of this tool can create, customize and even download a spreadsheet copy of the results. On April 04, 2023, the researcher began collecting data, and on April 20, 2023. The researcher facilitated the online form collection with proper consent from the respondents.

The researcher ensured the confidentiality of information given by the respondents. The collected data will be counted to ensure that the total number of needed samples is met. Then, the data collected will be tabulated, analyzed and assessed based on the result.

3.6 Statistical Treatment of Data

The statistical treatment of data was used to reflect the demographic profile of the respondents in terms of the frequency and percentage distribution that is presented in a graphical format.

Percentage Formula: P = n x 360

Where;

n= the particular number of respondents N= the total number of respondents

The study also used a **t-Test** to evaluate the data. The T-Test is a method for utilizing hypothesis testing to evaluate the means of one or two populations. prior to collecting data, we specify the level of probability (alpha level, level of significance, p) that we are willing to accept (p.05 is a common value). After gathering data, we use a formula to compute a test statistic. To determine whether our results are within an acceptable threshold of probability, we compare our test statistic to an essential number presented in a table.

3.7 Weighted Mean.

This was used to compute and determine the average response of the respondents on the various factors considered in the study. This statistical tool was used in answering the questions under the statement of problem #2. The formula is: For verbal interpretation of the computed weighted means, the following intervals were:

Weights Limits Verbal Interpretation

WM	Weighted mean	VI-verbal interpretation
3.26 – 4.00	Strongly Agree	(SA)
2.51 – 3.25	Agree	(A)
1.76 – 2.50	Disagree	(D)
1.00 – 1.75	Strongly Disagree	(SD)

Weights Limits Verbal Interpretation third part of the questionnaire.

WM	Weighted mean	VI-verbal interpretation
3.26 – 4.00	Very Serious	(VS)
2.51 – 3.25	Seiour	(S)
1.76 – 2.50	Disagree	(LS)
1.00 – 1.75	Strongly Disagree	(NS)

To determine the security measures of digital banking as the basis for improved security measures, the formula to be used to determine the weighted mean is:

$$X_N = \frac{\sum f_N}{N}$$

Where:

X_n= Weighted Mean

$\sum fn$= sum of all products of f & n

f= frequency of each weight

w= weight of each option

N= sum of all respondent

$$\Rightarrow F = \frac{MST}{MSE}$$

$$\Rightarrow F = \frac{\sum_{j=1}^{k} \sum_{j=1}^{l} (\bar{x}_j - x_j)^2}{df_w}$$

$$\Rightarrow F = \frac{\sum_{j=1}^{k} \sum_{j=1}^{l} (\bar{x}_j - x_j)^2}{k - 1}$$

Where,

x - The data points

$\bar{x}_j$ - The mean of the data points

df_w - The degrees of freedom for the data points within the range

4. Presentation, Analysis, and Interpretation of Data

This chapter presents and discusses the relevant results of the study vis-à-vis the statement of the problem and hypothesis. The discussion is divided in accordance with the sub-problems of the study.

4.1 Demographic Profile of the Respondents

4.1.1 Age;

Table 1. Demographic Profile of the Respondents in terms of Age

Indicators	Frequency	Percentage	Rank
18-25 years old	119	33.05	2
26-35 years old	215	59.72	1
36-45 years old	26	7.22	3
46-55 years old	0	0.00	4.5
56 years old and above	0	0.00	4.5
Total	**360**	**100.0**	

Table 1 presents the demographic profile of the respondents in terms of age. As shown in the table, the majority of the respondents belong to the age bracket of 26-35 years old, with 215 or 59.72 percent. Second, the highest number of respondents belonged to the age bracket of 18-25 years old or 119 or 33.05 percent. The third highest number of respondents is within the age bracket of 36-45 years old, with 26 or 7.22 percent.

The data shows that middle-aged individuals and millennials are everyday digital banking users. The millennials are those individuals who have access to digital applications and are knowledgeable in the security procedures and security features of mobile apps for digital banking services. The age of technology, or the digital age, is adopted by young generations in order to be flexible in transacting their business conveniently through mobile apps or websites.

Moreover, the age of the application users for digital banking services is one of the determinants of the level of knowledge on the functions and features of digital banking. In other words, younger people who are exposed to digital banking have more access to and knowledge about its security features. They usually explore all the features of the apps and digital banking services. Hence, they can trust digital banking, which is secured from possible fraud and hacking.

Compared to all older people who have limited knowledge and understanding about the utilization of digital applicants, they tend to transact their business at the bank and patiently wait to be called to be catered by the teller, compared to the young generation who conveniently transact business using online.

4.1.2 Sex;

Table 2. Demographic Profile of the Respondents in terms of Sex

Indicators	Frequency	Percentage	Rank
Male	155	43.06	2
Female	205	56.94	1
Total	**360**	**100.0**	

Table 2 presents the demographic profile of the respondents in terms of sex. As shown in the table, the majority of the respondents were female, with 205 or 56.94 percent, compared to male respondents, with 155 or 43.06 percent. This shows that the majority of digital banking users are women since they have more transactions than men. Moreover, women utilize commonly online applications together with digital banking in order to transact their purchases online.

Online payments such as bank transfers are required in order to purchase online. Hence, women are more aware of the security measures of the digital banking system compared to men, who commonly used electronic banking via ATM machines instead of doing transactions online. Men make direct purchases to the physical store.

4.1.3 Source of Income;

Table 3. Demographic Profile of the Respondents in terms of Source of Income

Indicators	Frequency	Percentage	Rank
Salary	324	90.00	1
Pension/Social Benefits	0	0	
Business Income	20	5.56	3.5

Dividend & Interest Payment	8	2.22	3.5
Funds From Family Members	8	2.22	3.5
Total	**360**	**100.0**	

Table 3 presents the demographic profile of the respondents in terms of source of income. As shown in the table, salary is the top source of income, which they transact using digital banking. Almost all respondents are totally dependent on their salary as the primary source of income.

Some respondents have their income from their business, which is comprised of 20 or 5.56 percent. The remaining respondents have their source of income from the dividend and interest payment of their investment, with a total of 8 or 2.22 percent. In addition, 8 respondents declared that the source of their income coming from the funds of the family members. This shows that the majority of digital banking users are employed and transact their business using digital banking to spend their salary.

There is no entry for pension or social benefits since, based on the demographic profile of the respondents, there are no respondents that fall under 56 years old and above, which are age.

4.1.4 Frequency of Usage of Digital Banking

Table 4. Demographic Profile of the Respondents in terms of Frequency of

Usage of Digital Banking

Indicators	Frequency	Percentage	Rank
Daily	134	37.22	1
Once a Week	122	33.89	2
Every two weeks	72	20.00	3
Once a month	14	3.89	4
Total	**18**	**5.00**	**5**

Table 4 presents the demographic profile of the respondents in terms of frequency of usage of digital banking. As shown in the table, the majority of the respondents utilized digital banking daily, with 134 or 37.22 percent. Some of them use it for online purchases through fund transfer transactions to meet their daily needs. Second to the highest users are those weekly or once a week, with a total of 122 or 33.89 percent. These users transact at digital banking in order to make necessary deposits or withdrawal transactions. In addition, 72 users or 20 percent, transact business using digital banking at least once a month for a deposit or their savings or checking their balances. Quarterly digital banking users, with a total of18 or 5 percent, make updates to their digital banking transactions.

4.2 Security Measures on Digital Banking

4.2.1 Trust and Security;

Table 5. Security Measures on Digital Banking in terms of Trust and Security

Indicators	WM	VI
1. Secured authentication method (ex., Face recognition, biometric, password)	3.62	SA
1. Can access multiple devices	2.97	A
2. Password protection	3.71	SA
3. Automatic attack detection blocking	3.39	SA
4. Strong transaction security	3.60	SA
5. Trusted hardware security	3.41	SA
6. Trusted hardware security	3.54	SA
7. File security	3.47	SA
OWM	**3.46**	**SA**

Legend: WM – Weighted Mean	**VI – Verbal Interpretation**

3.26 - 4.00	Strongly Agree	(SA)
2.51 – 3.25	Agree	(A)
1.76 – 2.50	Disagree	(D)
1.00 – 1.75	Strongly Disagree	(SD)

Table 5 reveals the respondents' assessments of security measures in digital banking in terms of trust and security. In the assessment of customer respondents, it was found that the indicator-secured password protection obtained the highest verbal interpretation of "strongly agree", with a weighted mean of 3.71. Six other indicators were rated by the customer respondents as "strongly agree". These mentioned indicators were authentication method (ex., Face recognition, biometric, password); automatic attack detection blocking; strong transaction security; trusted hardware security; confidentiality; and file security, obtained weighted means of 3.62, 3.39, 3.60, 3.41, 3.54, and 3.47, respectively. The indicator can access multiple devices was rated as "agree", with the lowest weighted mean of 2.97. The overall rating given by the respondents is "strongly agree," with a weighted mean of 3. 46.

The result implies that respondents considered trust and security in the utilization of digital banking applications to be very important in order toattract customers to shift to digital banking instead of visiting a branch.

However, the least trust of the customers in the security measures of digital banking is the accessibility using multiple devices. Accessing digital banking through recognized and registered mobile devices allow users to access -information and transact business using digital banking application. In relation to the findings, the issue of trust and security in the utilization of digital banking, Vejačk (2021) found out that the security measures play an important role in winning the trust of individuals. The important issue is the trust of bank customers in the form of electronic banking used.

Banks' customers also sensitively perceive the security of electronic banking forms used by them. In this article, we mainly investigated the influence of security and trust on electronic banking adoption. A research model based on the technology acceptance model was developed, and research hypotheses based on this research model were constructed. The results reveal that all factors investigated have statistically significant direct and indirect effects on electronic banking adoption by users in the retail banking market.

Moreover, in support of the claims of the reviewed studies on security and trust to the security measures of digital baking, Gabriel (2023) presented the influence of privacy of digital banking on the trust of the users. According to him, the growth and development of technology in recent times and the increased use of digital platforms by companies have set a new course in the work and personal lives of workers and users. This digital shift has revolutionized consumer behavior and commercial exchanges, where e-commerce is positioned at its peak.

4.2.2 Knowledge and Awareness;

Table 6. Security Measures on Digital Banking in terms of Knowledge and Awareness

Indicators	WM	VI
1. Assurance of the confidentiality of information	3.61	SA
2. Security reminders for possible fraud or hacking	3.50	SA
3. Importance of securing one time password (OTP)	3.70	SA
4. Notice for the utilization of the unsecured websites	3.38	SA
5. Notice for the utilization of the unsecured websites	3.45	SA
6. Provide information on different authentication channels (ex., Biometrics, finger scan) and application update	3.46	SA
7. Instruction for registration, recovery or change of user account and password	3.48	SA
8. Instruction of application features and proper usage	3.24	A
OWM	**3.48**	**SA**

Legend: WM – Weighted Mean	VI – Verbal Interpretation	
3.26 - 4.00	Strongly Agree	(SA)
2.51 – 3.25	Agree	(A)

1.76 – 2.50	Disagree	(D)
1.00 – 1.75	Strongly Disagree	(SD)

Table 6 shows the respondents' assessments of security measures in digital banking in terms of knowledge and awareness.

In the assessment of customer respondents, it was found that the indicator importance of securing one time password (OTP) obtained the highest verbal interpretation of "strongly agree" with a weighted mean of 3.70. Seven other indicators were rated by the customer respondents as "strongly agree". These mentioned indicators were assurance on the confidentiality of information; security reminders for possible fraud or hacking; notice for the utilization of unsecured websites; warning for input of credentials; provide information of different authentication channels (ex., Biometrics, finger scan) and application update; instruction for registration, recovery or change of user account and password; and Instruction for registration, recovery or change of user account and password obtained weighted means of 3.61, 3.50, 3.38, 3.45, 3.46, 3.48, and 3.24, respectively. The indicator notice for the Instruction of application features and proper usage was rated as "Agree", with the lowest weighted mean of 3.24. The overall rating given by the respondents is "strongly agree", with a weighted mean of 3.48.

The outcome of the study reveals that the respondents are knowledgeable and aware of the security measures and security features of digital baking. This is one of the reasons why they continuously use online or digital banking aside from the convenience and flexibility in transacting business.

The level of knowledge and awareness of the customers in the utilization of online banking encourage the users and other bank customers to transact business in any channel using digital banking.

Moreover, in the study on awareness, utilization and barriers to the ebanking system, Kaur (2020) explain the primary purpose of the e-banking system. E-banking is electronic banking that provides financial services for individual clients by means of the Internet. E-banking includes the systems that enable financial institution customers, individuals or businesses to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet.

In addition, according to Shaji (2020), the revolution in electronic technology has taken the world. The banking sector has not been immune to the impact of this digital revolution. In India, both private and public banks have changed their standard business practices and have now shifted entirely to electronic banking. The banking transactions that are executed through electronic devices and over the internet are termed electronic banking. One of the special features of urbanization is that urbanized society, irrespective of gender, is ready to accept the change and adjust to the new technologies quickly because of their extensive exposure to these innovations and their higher educational standard.

Hence, the utilization of electronic banking increases the level of progress and speed in transacting business in the bank due to alternative banking channels.

4.2.3. Ease to Use;

Table 7. Security Measures on Digital Banking in terms of Ease of Use

Indicators	WM	VI
1. Easy access to the mobile banking application	3.51	SA
2. Easy withdrawal transactions	3.59	SA
3. Time-saving and anytime banking	3.62	SA
4. Ease of monitoring of accounts and transactions	3.63	SA
5. Convenience in doing business transactions in apps	3.59	SA
6. Create a seamless app experience for users & prompt customer service	3.52	SA
7. QR Code generation for faster fund transfer & other easy access for self-service facility	3.57	SA
8. Imposing cheaper fee in every transaction (Fund transfer, Bills payment, etc.)	3.30	SA
OWM	**3.59**	**SA**

Legend: WM – Weighted Mean	**VI – Verbal Interpretation**	
3.26 - 4.00	Strongly Agree	(SA)
2.51 – 3.25	Agree	(A)

1.76 – 2.50	Disagree	(D)
1.00 – 1.75	Strongly Disagree	(SD)

Table 7 demonstrates the respondents' assessments of security measures on digital banking in terms of ease of use. In the assessment of customer respondents, it was found that the indicators time saving and anytime banking and ease of monitoring of accounts and transactionsobtained the highest verbal interpretation of "strongly agree", with a weighted mean of 3.63. Six other indicators were rated by the customer respondents as "strongly agree". These mentioned indicators were easy access to mobile banking applications, easy withdrawal transactions, convenience in doing business transactions in apps; create a seamless app experience for users & prompt customer service, QR code generation for faster fund transfer & other easy access for the self-service facility; and imposing cheaper fee in every transaction (Fund transfer, Bills payment, etc.) Obtained weighted means of 3.51, 3.59, 3.62, 3.59, 3.52, and 3.57, respectively. The indicator Imposing cheaper fee in every transaction were rated as "strongly agree", with the lowest weighted mean of 3.30. The overall rating given by the respondents is "strongly agree", with a weighted mean of 3. 59.

The result implies that the digital banking experience is more convenient on the part of the customers, particularly in the withdrawal of their salary using the Automated Teller Machine. The availability of ATMs allows for the flexibility of banking experience.

In support of this finding, the security measures of the digital banking system enable the customer to use it with easiness and accessibility to all with its user-friendly features. In the study of Asif (2021) on Internet banking usage between the elderly and youth, findings indicate that there is a relationship between the experience of online banking and the experience of traditional banking. The findings also reveal that there is enough evidence to support that there is a relationship between no. Of years of usage and online banking. In this research, it is seen that internet banking is majorly used by the youth instead of visiting banks. Whereas old people prefer visiting physically to banks as earlier in their time, there was no internet banking used that much as compared to this time.

Moreover, Salihu (2019) on the effect of security and ease of use on reducing problems of electronic banking services, the use of technology in banking operations has facilitated many daily banking activities. However, the use of technology in electronic banking services has its problems/deficiencies as well.

Titus (2021) on the customer perception of ease of use of internet banking, Internet banking allows banks to provide information and offer services to their customers conveniently using the internet technology. However, studies have shown that customers have perceptions that impact the uptake and continuous usage of the platform.

4.2.4 Usefulness;

Table 8. Security Measures on Digital Banking in terms of Usefulness

Indicators	WM	VI
1. Secured digital banking transactions	3.57	SA
2. Quick settlement of obligations	3.52	SA
3. Electronic bill payment and clearing services	3.64	SA
4. Checkbook requisition and other service request clearing services	3.36	SA
5. Access to fund transfer to own, third-party & other banks (Insta pay & Peso net)	3.51	SA
6. Quality of bank transaction services	3.49	SA
7. Various security features to protect bank account	3.54	SA
8. Generate bank statement through application	3.42	SA
OWM	**3.51**	**SA**

Legend: WM – Weighted Mean	VI – Verbal Interpretation	
3.26 - 4.00	Strongly Agree	(SA)
2.51 – 3.25	Agree	(A)
1.76 – 2.50	Disagree	(D)
1.00 – 1.75	Strongly Disagree	(SD)

Table 8 reveals the respondents' assessments of security measures in digital banking in terms of usefulness. In the assessment of customer respondents, it was found that the indicator electronic bills payment and clearing services obtained the highest verbal

interpretation of "strongly agree", with a weighted mean of 3.64. Seven other indicators were rated by the customer respondents as"strongly agree". These mentioned indicators were secured digital banking transactions; quick settlement of obligations; checkbook requisition and other service request clearing services; access to fund transfer to own, third-party & other banks (Insta pay & Peso net); quality of bank transaction services; various security features to protect bank account; and generate bank statement through application obtained weighted means of 3.57, 3.52 3.51, 3.49, 3.54, and 3.42, respectively. The indicator for checkbook requisition and other service request clearing services was rated as "strongly agree", with the lowest weighted mean of 3.36. The overall rating given by the respondents is "strongly agree," with a weighted mean of 3. 51. This study reveals that respondents considered digital banking is very useful to their regular customers in transacting business. The security features and other functions or features of the banks allow them to utilize them based on their desired transactions. They can easily transfer, pay, and deposit money anytime and anywhere. Similar to other studies, In Malaysia, the study of Ali (2020) revealed the consumers perceived ease of use and trust in online banking. According to him, the development and invention of technology has transformed the way organizations conduct their businesses currently, including banking institutions, mainly in offering online banking services. Online banking services have been introduced in Malaysia. Still, online banking users in Malaysia are intolerant of issues of trust towards online banking, which affect their level of acceptance. The findings showed that perceived ease of use and trust have a significant relationship with the intention to use internet banking. Moreover, One of the key benefits or advantages of the utilization of digital banking, according to Rebello (2022), the digital banking can be described as the digitization or automation of almost all traditional banking activities and services, such as money transfers, making payments, checking the account balance and more with the use of secured digital channels. These banking activities and services were previously accessible only at the bank branch.

Furthermore, with digital banking, customers can use digital wallets, online banking facilities, mobile apps for payments, and do much more. The rise of technology in the past 20 years has brought unprecedented changes to the world of banking. People can use the Internet to perform various banking transactions with ease.

4.3 Significant Difference in the Assessment of the Respondents on the Security Measures of Digital Banking when Grouped According to Profile

Table 9. Result of Test of Significant Difference on the Assessment of the Respondents on the Security Measures on Digital Banking when Grouped According to Profile

Variable	T-Computed	T-Tabular	Decision on HO	Interpretation
1. Trust and Security	2.012	1.936	Reject	Significant
2. Knowledge and Awareness	2.115	1.936	Reject	Significant
3. Ease to use	2.052	1.936	Reject	Significant
4. Usefulness	2.152	1.936	Reject	Significant
Level of Significance	**0.05**			

The result of a test of significant difference in the respondents' evaluation of the security measures of digital banking in terms of trust and security, knowledge and awareness, ease of use, and usefulness when they are grouped according to their profile is shown in Table 9. The statistical test using a t-test showed that the computed t-values of 2.012, 2.115, 2.052, and 2.152 are greater than the tabular t- value of 1.936 (two tail), indicating the acceptance of the null hypothesis. Thus, the statistics revealed that there is a significant difference in the evaluation of the two groups of respondents with respect to the level of security measures on digital banking and their profiles. The results show that the respondents have different perception of the level of security measures of digital banking when age, sex, source of income, and frequency of usage of digital banking is concern. This further show that the gender preference or sexes of digital banking users have a different perception of the security measures of digital banking. The level of trust and confidence, level of awareness and knowledge of digital banking varies in the ages of the users and the frequency of the utilization of that platform in banking transactions.

In support of these findings, Rendell (2022) presented the important reasons why banks must increase their focus on developing digital trust. Fraudsters are targeting the end consumer. Banks have invested in fraud detection solutions that have made it harder for criminals to commit fraud. As a result, fraudsters are focusing their attention on the next most vulnerable cog in the transaction: the end consumer. Fraudsters might prey upon potential victims during a moment of weakness like a medical situation or by taking

advantage of world events like the pandemic to push a scam. the bank will have to take measures to authenticate the customer at multiple steps of their journey. Too much intervention leaves customers feeling irritated and annoyed at their bank.

4.4 Common Digital Banking Issues or Problems Encountered by the Respondent

Table 10. Common Digital Banking Issues or Problems Encountered by the Respondents

Indicators	**WM**	**VI**
1. Changing or forgetting password	3.08	S
2. Slow process of transaction	2.84	S
3. Slow process of transaction	2.56	S
4. Possible hacking of account	3.19	S
5. No regular updates of the system	2.53	S
6. Inadequate response of the customer service	2.78	S
7. Problems in navigating the application	2.70	S
8. Lack of safety and security reminders	1.00	NS
9. Offline and technical problems often encountered	2.91	S
10. Offline and technical problems often encountered	2.62	S
OWM	**2.62**	**S**

Legend: WM – Weighted Mean	**VI – Verbal Interpretation**	
3.26 - 4.00	Very Serious	(VS)
2.51 – 3.25	Serious	(S)
1.76 – 2.50	Less Serious	(LS)
1.00 – 1.75	Not Serious	(NS)

Table 10 reveals the respondents' assessments of common digital banking issues or problems encountered by the respondents. In the assessment of customer respondents, it was found that the indicator Possible hacking of account obtained the highest verbal interpretation of "serious", with a weighted mean of 3.19. Eight other indicators were rated by the customer respondents as "serious". These mentioned indicators were changing or forgetting passwords, slow process of transaction, no regular update of the system, inadequate response of the customer service, problems in navigating the application, and security reminders, offline and technical problems often encountered, and limited access to digital banking transactions obtained weighted means of 3.08,2.84, 2.56, 2.53, 2.78, 2.70,2.91 and 2.62, respectively. The indicator Lack of safety and security reminders was rated as "less serious", with a lowest weighted mean of 1.00. The overall rating given by the respondents is "serious", with the obtained weighted mean of 2.62.

The result implies that the problems encountered by the digital banking user concerning the security measures of digital banking is serious, particularly the problem with regard to Possible hacking of account.

Thus, despite the high security measures in the utilization of digital banking, they encounter serious problems in its actual utilization due to the technical difficulty of the users in handling such acts.

4.5 Output as the Basis of Improvement of Digital Banking

Area of Concern	Findings of the Study	Possible for Improvement	Possible Outcome
Trust and Security	The least rating on the security measure is the access using multiple devices	Limit the simultaneous usage of digital banking using multiple devices	Access to single device to avoid multiple logs
Knowledge and Awareness	The least rating on the security measure is giving Instructions of application features and proper usage	Provide digital banking user a clear periodic email and SMS blast for any updated about features of digital banking and security reminders	Digital banking users will be more informed about the new features and proper usage of digital banking.
Ease of Use	The least security measures are the imposition of cheaper fee in every transaction (Fund transfer, Bills payment etc.)	Gradually increase the convenience fee in order to limit multiple transactions in a day	Utilize the digital banking activities in order prevents multiple transaction in every single account of users
Usefulness	Utilize the digital banking activities in order prevent multiple transaction in every single account of users	Modification of the bank policy on the clearing services	One day clearing process is applied in all transactions
Encountered Concerns on the Security Measures	The most serious issues on security measures are possible hacking of account	Provide the digital banking users with the strict reminders about giving account information to unreliable person/sources	Digital banking users will become more vigilant in giving confidential information such as OTP.

5. Summary of Findings, Conclusions and Recommendations

This chapter presents the summary of the findings, conclusions, and recommendations on the assessment of the security measures in digital banking.

The study aimed to assess the level of security measures in digital banking in terms of trust and security, knowledge and awareness, ease of use, and usefulness. Further, it determined whether there is a significant difference in the assessment of the significant difference on the assessment of the respondents on the security measures of digital banking when grouped according to profile. Moreover, the output of the study as a basis for improvement is based on the results of the study.

This study made used of three hundred sixty (360) respondents. The survey questionnaire was used as the main gathering instrument for the acquisition of the needed data. Also, it includes the average weighted mean and T-Test as statistical tools. The study was conducted in Metro Manila using online applications such as google forms.

5.1 Summary of Findings

1. Demographic Profile of the Respondents

The demographic profile of the digital baking users as the respondents of the study revealed that the majority of the respondents belong to the age bracket between 26 to 35 years old. Most of them are female. Almost all of them utilized digital banking in spending their salary. In addition, the majority of the respondents are daily users of digital banking.

5.2 Security Measures of Security Measures on Digital Banking

5.2.1. Trust and Security

The respondents assessed the security measures on digital banking in terms of trust and security as strongly agree, as manifested by the obtained overall weighted mean of 3.36. The indicator can access multiple devices obtained the least rating of 2.97, which is equivalent to agree.

5.2.2. Knowledge and Awareness

The respondents assessed the security measures on digital banking in terms of knowledge and awareness as strongly agree, as manifested by the obtained overall weighted mean of 3.48. The indicators Instruction of application features and proper usage obtained the least rating of 3.24, which is interpreted as strongly agree.

5.2.3. Ease of Use

The respondents assessed the security measures on digital banking in terms of ease of use as strongly agree, as manifested by the obtained overall weighted mean of 3.59. The indicator Imposing cheaper fee in every transaction obtained the least rating of 3.30, which is equivalent to strongly agree.

5.2.4. Usefulness

The respondents assessed the security measures on digital banking in terms of usefulness as strongly agree, as manifested by the obtained overall weighted mean of 3.51. The indicator checkbook requisition and other service request clearing services obtained the least rating of 3.36, Which is equivalent to strongly agree.

5.3 Significant Difference in the Assessment of the Respondents on the Security Measures of Digital Banking when Grouped According to Profile

The assessment of respondents revealed that there is no significant difference in the assessment of the respondents on the security measures of digital banking when grouped according to profile, as manifested by the computed t-values of 2.012, 2.115, 2.052, and 2.152, which is greater than the critical t-value of 1.936; thus the null hypothesis is rejected.

5.4 Common Digital Banking Issues or Problems Encountered by the Respondents

The respondents assessed the common digital banking issues or problems encountered by the respondents as serious, as manifested by the obtained overall weighted mean of 2.62. The indicator Possible hacking of account obtained the highest rating of 3.9, which is interpreted as serious.

The output of the study as a basis for improvement includes the following:
Access using multiple devices; imposition of cheaper fee in every transaction; Instruction of application features and proper usage; possible hacking of account and checkbook requisition and other service request clearing services.

5.5 Conclusions

Based on the findings, the following conclusions are drawn:

1. The demographic profile of the respondents revealed that the majority of the online users are young individuals who usually stay at home or their workplace to transact business using online banking to spend their salary for buying personal needs. They utilized digital banking on a daily basis.
2. The security measures on digital banking in terms of trust and security trust and security, knowledge and awareness, ease of use, and usefulness are strongly agreed upon. However, it is necessary to improve the security measures with regard to accessing the apps using multiple devices, securing one time passwords, an easy withdrawal system, and clearing service requests.
3. There is a similarity in the assessment of the respondents on the security measures of digital banking when grouped according to profile
4. The common digital banking issues or problems encountered by the respondents is serious, particularly the Possible hacking of account, which is a threat to the users and imposed doubt about continuously using digital banking.

5.6 Recommendations

Based on the findings and conclusions, the following are recommended:
1. The digital banking administrator should limit the simultaneous usage of digital banking using multiple devices.

2. The Central Bank of China should moderate the increase in the convenience fee in order to limit multiple transactions in a day
3. The bankers should increase the periodic email and sms blasts as well as social media reminders about Instruction on application features and proper usage.
4. The banks should increase the level of confidence of digital banking users by providing information and reminders about being more vigilant about sharing personal data. As well as increasing and investing in the security measures of the banks.
5. Further study should be conducted concerning the factors affecting the digital banking users on their trust and confidence in the utilization of digital banking as support to the present study.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Ali, S R O (2020). Perceived Ease of Use and Trust Towards Intention to Use Online Banking in Malaysia. DOI:10.24191/ji.v15i1.273
[2] Amtul, F (2020). The E-banking Security Issue. Scholar, Jawaharlal University of Technological studies, A.P., India. https://www.icommercecentral.com/open-access/ebanking-securityissues-is-there-a-solution-in biometrics.php?aid=38240
[3] Anene, I A. and Okeji, C C. PhD, (2021).Awareness, Acceptance and Usage of Mobile Banking Services by Academic Librarians in Nigeria. Library Philosophy and Practice (e-journal). 4986. https://digitalcommons.unl.edu/libphilprac/4986
[4] Asif, S (2021). Study Of Internet Banking Usage: Elderly Vs Youth. Centre for Innovation & Entrepreneurship, GD Goenka University. Ilkogretim Online - Elementary Education Online, Vol 20 (Issue 6): pp. 3086-3101. http://ilkogretim-online.org. doi: 10.17051/ilkonline.2021.06.287
[5] Bansal, K M (2020). Cyber Security Issues Affecting Online Banking Transaction: A Thematic Analysis. Department of Commerce B. R. Ambedkar. College, (University of Delhi) Ilkogretim Online - Elementary Education Online, 19 (Issue 4): . 7724-7740. http://ilkogretimonline.org; doi: 10.17051/ilkonline.2020.04.765171
[6] Belás, J.; Korauš, M.; Kombo, F.; Korauš. A. (2016). Electronic banking security and customer satisfaction and in commercial banks, *Journal of Security and Sustainability Issues* 5(3): 411–422. DOI: http://dx.doi.org/10.9770/jssi.2016.5.3(9)65
[7] Brundel C., & Azrioua S. (May 2018) The Acceptance of Mobile Banking by Organizationshttp://hj.divaportal.org/smash/get/diva2:1214186/FULLTEXT 01.pdf
[8] Chinabank Corporation https://www.chinabank.ph/about_china_bank.aspx
[9] Eastwesthttps://www.eastwestbanker.com/about/whoweare https://www.cc.gatech.edu/gvu/user_surveys/survey-199804/questions/ banking.htm
[10] Gabriel, J, Martínez-Navalón, M Fernández-Fernández & Fernanda P A (2023). Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal*? International Entrepreneurship and Management Journal.* https://link.springer.com/article/10.1007/s11365-023-00839-4
[11] Gartner (2019). *Gartner Predicts Indian Banking and Securities IT*: https://www.gartner.com/en/newsroom/press-releases/2019-06-18-gartner-predicts-indian-banking-and-securities-it-spe
[12] Kaur, K (2020). A Study on Awareness, Utilization and Barriers towards EBanking in East Delhi, India*. International Journal of Innovative Studies in Sociology and Humanities* (IJISSH) 1 : 1.
[13] Kiran, J (2022). Customer Awareness and Preference for the Digital Banking Offered by the HDFC Bank: An Empirical Study. Department of Commerce, MCM DAV College for Women, Chandigarh, India
[14] Mohan, Dr. Madana M (2022). Factors Influencing Customers To Use Digital Banking Services In Twin Cities Of Telangana State. Vishwani School of Business, Thumkunta, Hyderabad.
[15] Moscato, D R. and Altschuller, S (2022) International Perceptions of Online Banking Security Concerns, Communications of the IIMA: 12: 3, Article 4. DOI: https://doi.org/10.58729/1941-6687.119366
[16] Nwaiwu, F, Michael K, Abdul J, Ladislav B, and Michal P. (2020) Impact of Security and Trust as Factors That Influence the Adoption and Use of Digital Technologies That Generate, Collect and Transmit User Data. International Conference on Cyber Warfare and Security, January, 363.
[17] PYMNTS (2023). Half of Consumers Want More Security Measures from Banks. Retrieved from: https://www.pymnts.com/authentication/2023/half-of consumers-want-more-security-measures-from-banks/
[18] PWC (2021) Digital Banking Consumer Survey. https://www.pwc.com/us/en/industries/financialservices/library/digitalban king-consumer-survey.html Rebello,
[19] Roshel (2022). What Is Digital Banking? https://www1.ipb.citibank.com.sg/en/wealthmatters/finance101/what-is digital-banking
[20] Rendell, R (2022). Why Digital Trust Should Be a Top Priority For Banks. https://www.paymentsjournal.com/why-digital-trust-should-be-a-toppriority-for-banks/
[21] Salihu, A (2019). The Effect of Security and Ease of Use on reducing the problems/deficiencies of Electronic Banking Services. IFAC-Papers On Line 52, 25, 159-163
[22] Shaji A K. (2020). A Study of the Awareness of Electronic Banking Services among Rural Women of Nelamangala, Bangalore, India. *Journal of International Women's Studies.* 67

[23] Southeast Asian fintech firm BigPay hints at Philippine launch. https://theindependentinvestor.ph/southeast-asian-fintech-firm-bigpay-hints-atphilippine-launch/
[24] Shanmugapriya, B. (2021). Study on Customer Awareness Towards Digital Banking Services". The Madura College https://www.researchgate.net/publication/354897738_
[25] Smith,D (2019). Security Vulnerabilities of Electronic Banking. Retrieved from https://www.asiapacificsecuritymagazine.com/5-securityvulnerabilities-of-electronic-banking/
[26] Subsorn P. (2022). Internet Banking Security in Thailand: A Customer Perspective. Procedia Engineering. 32, 2022, 260-272 https://doi.org/10.1016/j.proeng.2012.01.1266
[27] Thomas, S S (2021). A Study on Awareness Towards Internet Banking Among Senior Citizens with Special Reference to Coimbatore City. *International Journal on Multi-Disciplinary Educational Research.* ISSN:2277-7881; IMPACT FACTOR :7.816; IC VALUE:5.16; ISI VALUE:2.286 DOI: http://ijmer.in.doi./2021/10.05.21
[28] Titus, S (2021). Customers Perception on Ease of Use of Internet Banking in Commercial Banks in Kenya. *International Journal of Novel Research in Marketing Management and Economics* 2, 2. Department of Computing and Information Technology Kenyatta University, Kenya.
[29] Vejačk, M (2021). Influence of security and trust on electronic banking adoption in Slovakia. The Technical University of Kosic. M: Ekonomie a Management 20(4):135-150. DOI:10.15240/tul/001-4-01068
[30] *What is Data Privacy*. SNIA: https://www.snia.org/education/what-is-data-privacy *Corporate Profile.* BDO https://www.bdo.com.ph/about-bdo/business operations#corporate_profile BPI https://www. bpi.com. ph/ Metrobank https://www.metrobank. com. ph/about-us