IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

A Study on Online Banking and Threat to the Personal Banking Information in Chennai

Vaishaali R
B.B.A LLB (Hons) 5th year
Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai
vaishaaliravichandran22@gmail.com

Abstract: *Online banking has revolutionised the way individuals manage their finances by offering the convenience of accessing banking services anytime and from anywhere. With just a few clicks, users can perform a range of financial transactions, from transferring funds to paying bills. However, this convenience comes with its own set of risks. Online transactions are susceptible to various security threats, including hacking, phishing, and data breaches. Although well-established financial institutions have implemented a wide array of advanced security measures to safeguard their users, it is equally important for individuals to adopt responsible practices to protect their financial and personal information. This study employs an empirical methodology to explore public awareness regarding the security threats associated with online banking. The research was conducted with a sample size of 211 participants, all from the Chennai region. The primary objective of this study is to assess whether the general public is adequately informed about the severity of the threats posed by online banking and the potential compromise of personal information. Based on the findings, it can be concluded that there has been a noticeable increase in the use of online banking services. Alongside this growth, the threat to personal information remains significant. Despite rigorous precautions and security protocols, the risk cannot be entirely eliminated, as online banking inevitably requires the sharing of sensitive personal data. Therefore, heightened awareness and cautious online behavior are crucial for ensuring safer digital financial transactions.*

Keywords: Online, information, banking, threat, personal

I. INTRODUCTION

Digital banking (online and mobile banking) makes managing finances easy. With digital banking technology, you can pay bills, deposit checks and transfer money from wherever you're located. Due largely to their convenience, online and mobile banking are the two most popular ways to bank. Online Banking offers users the convenience of managing one's finances anytime, anywhere. However, any online transaction can be vulnerable to security threats. While reputable financial institutions implement a slew of security measures, you can take some steps on your own to keep your financial and personal details out of the hands of hackers. Some financial institutions today still employ simple security mechanisms that consist of a username and password combination for login and money transfers. These are easily breached by the increasingly sophisticated methods fraudsters use and have resulted in users having their account details compromised. Online banking is becoming increasingly popular as it brings convenience, simplicity and speed to consumers. Common techniques deployed by fraudsters today to obtain login credentials for users' online banking accounts include phishing, pharming, keylogging, man-in-the-middle and man-in-the-browser attacks. Regardless of the method employed, fraud is a global phenomenon that is constantly evolving in order to exploit security gaps. It also possesses a migratory nature, targeting countries which have less sophisticated security infrastructure. To prevent and deter fraud, banks must be ahead of the curve through regular upgrading of its infrastructure. No matter how much precautions banks take to provide a secure network, online banking transactions are still susceptible to hackers. Irrespective of the advanced encryption methods used to keep user data safe, there have been cases where the transaction data is compromised. This may cause a major threat such as using the data illegally for the hacker's benefit.

DOI: 10.48175/IJARSCT-27544

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, June 2025 Impact Factor: 7.67

Large-scale data breaches get the headlines, but criminals also work on a smaller scale by attacking consumers directly. For example, fraudsters often use so-called phishing scams, in which they send out emails or text messages pretending to represent a financial institution in the hopes of hooking an unsuspecting consumer. However, implementing security measures for online banking is a task that's easier said than done. Securing an online banking channel has many aspects to it and each needs to be addressed individually. A key challenge faced by banks when upgrading their security infrastructure is identifying which technologies to adopt and which parts of their infrastructure to change or upgrade. Apart from having to provide a robust and secure channel for online banking, banks need to decide on a solution that not only suits theirneeds, but also balances security, cost and convenience for their customers. To combat these concerns and protect your cash, banks and credit unions employ policies to keep online customer accounts secure. Standard measures include using anti-virus protection on bank computers, firewalls, fraud monitoring and website encryption, which scrambles data so only the intended recipient can read it. If you bank online, chances are your financial institution uses these security measures. Due to lockdown restrictions, online banking adoption soared and now up to 80% of people prefer online banking to visiting the bank, and banks all over the world have started closing the doors of their physical branches. Further to this increase in digital banking usage has been an increase in contactless solutions amidst social distancing practices.

OBJECTIVES:

- To analyze if there is a threat to personal information due to online banking
- To study the impact of threat caused due to personal banking information
- To study the rise of online banking transaction and safety of personal information

II. REVIEW OF LITERATURE:

Cybercrime is a bigger risk now than ever. Illegal activities conducted by cyber fraudsters and criminals using electronic means such as computers, mobiles and other network devices are genus of crimes which are transitional in nature compared to traditional crimes. Cyber criminals use a number of methods depending on their skills set and their goals and objectives. The importance of additional security devices to enhance the levels of security of online banking is also discussed.**(Lucas 2017)** Customers' behaviour plays an important role in combattingonline-banking fraud. This study develops a model of precautionary online behaviour in the domain of online banking, based on protection motivation theory and other behavioural models. The model was tested with questionnaire data of 1200 users of online banking services in the Netherlands. Results from partial-least-squares path-modelling provide support for most hypothesized relationships and show that the model explains high levels of variance for precautionary online behaviour as well as for risk perception. The outcomes of this study can be used by scholars and information-security professionals to improve security education, training and awareness campaigns directed at safe online banking.**(Arezes 2018)** Online banking faces different kinds of risks that are specific to conducting sensitive business over the Internet. It is imperative that banks implement strong security approaches that can adequately address, monitor, manage, and control risks and security threats. This paper demonstrates that online banking may confront operational, security, legal, and reputation risks. **(National Research Council et al. 1997)** This study examines the relationship between perceived security and acceptance of online banking with the mediating effect of perceived risk and trust in Internet banking in Iranian customers. Researchers used structural equations models (SEM) to examine their hypotheses and conceptual models. Statistical data were gathered via a questionnaire from 395 randomly selected customers of Bank Saderat Iran in Semnan. Cronbach's alpha and internal compatibility were used to check the reliability of the questionnaire. The justifiability of the research variables was checked and confirmed using the first- and second-order confirmatory factor analysis.(**National Research Council et al. 1997**; Davis, Granic, and Marangunic 2020 The main purpose of this paper is to extend the technology acceptance model (TAM) in the context of internet banking adoption in India under security and privacythreat.Keeping the TAM proposed by Davis as a theoretical basis, an extended TAM incorporating security- and privacy-related issues for internet banking adoption is conceptualized. The paper reveals that perceived risk has a negative impact on behavioral intention of internet banking adoption and trust has a negative impact on perceived risk. A well-designed web site was also found to be helpful in facilitating easier use and also minimizing perceived risk

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

concerns regarding internet banking usage.**(Kesharwani and Bisht 2012** Adopting the technology acceptance model, this research examines the factors that determine intention to use online banking in Malaysia Borneo. Perceived ease of use and perceived usefulness factors are considered to be fundamental in determining the acceptance and use of various information technologies. However, these beliefs may not fully clarify behavioural intention towards newly emerging technologies, such as online banking.This study extends the model to include user computer experience and confidence.mThe results indicate that perceived usefulness and perceived ease of use are strong determinants of behavioural intention to adopt online banking. There is also an indirect effect of computer self-efficacy and prior general computing experience on behavioural intention through perceived usefulness and perceived ease of use the relatively small size of the sample somewhat limits generalizations.**(Guriting and Ndubisi 2006)** Online banking has become increasingly important to the profitability of financial institutions as well as adding convenience for their customers. As the number of customers using online banking increases, online banking systems are becoming more desirable targets for criminals to attack. To maintain their customers' trust and confidence in the security of their online bank accounts, financial institutions must identify how attackers compromise accounts and develop methods to protect them. Attack trees and protection trees are a cost effective way to do this. Attack trees highlight the weaknesses in a system and protection trees provide a methodical means of mitigating these weaknesses. In this paper, a notional online banking system is analyzed and protection solutions are proposed for varying budgets(**Guriting and Ndubisi 2006; Edge et al. 2007**) South Africa has a well-developed and established banking system which compares favourably with those in many developed countries (e.g. USA), but also sets South Africa apart from many other emerging market countries like Egypt and Brazil. Fourdominant banks, namely the Amalgamated Banks of South Africa **(ABSA)**, Standard Bank, Nedcor and First National Bank (FNB) influence the South African banking environment. **(Clark et 2009)** This paper reports key findings from an interpretive study of Australian banking consumer experiences with the adoption of internet banking. The paper provides an understanding of how and why specific factors affect the consumer decision whether or not to bank on the internet, in the Australian context. A theoretical framework is provided that conceptualizes and links consumer-oriented issues influencing adoption of internet banking. The paper also provides a set of recommendations for Australian banks. Specifically, the findings suggest that convenience is the main motivator for consumers to bank on the internet, while there are a range of other influential factors that may be modulated by banks. **(Karanovic, Polychronidou, and Karasavvoglou 2022)** One of the major issues banks are faced with in providing Internet Banking (IB) services is the adoption of these services by the customers. This study seeks to answer the question that whether bank customers' awareness of the services and advantages of IB is effective in reducing the negative effect of customers' are simultaneously considered. Besides, in the research model, the effect of IB awareness on each dimension of the perceived risk and the effect of these dimensions on intention of IB adoption by the customers are investigated.**(Hanafizadeh and Khedmatgozar 2012)** Internet banking is changing the banking industry, having the major effects on banking relationships. Banking is now no longer confined to the branches were one has to approach the branch in person, to withdraw cash or deposit a cheque or request a statement of accounts. In true Internet banking, any inquiry or transaction is processed online without any reference to the branch (anywhere banking) at any time. Providing Internet banking is increasingly becoming a "need to have" than a "nice to have" service. **(Hanafizadeh 2018)** In this paper the competitive landscape of financial institutions is shifting and internet banking is no longer a competitive advantage but a competitive necessity for banks. However, a limited number of empirical studies have been published in the marketing literature about electronic banking. This paper seeks to examine consumers' choices between electronic banking and non-electronic banking in New Zealand.**(shilpan Dineshkumar 2019)** Online banking (Internet banking) has emerged as one of the most profitable e-commerce applications over the last decade. Although several prior research projects have focused on the factors that impact on the adoption of information technology or Internet, there is limited empirical work which simultaneously captures the success factors (positive factors) andresistance factors (negative factors) that help customers to adopt online banking. This paper explores and integrates the various advantages of online banking to form a positive factor. **(Zeland Christoper 2001)** Understanding the main determinants of Internet banking adoption is important for banks and users; our understanding of the role of users' perceived risk in Internet banking adoption is limited. In response, we develop a conceptual model that combines unified theory of acceptance and use of technology **(UTAUT)** with perceived risk to explain behaviour intention and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, June 2025 Impact Factor: 7.67

usage behaviour of Internet banking.(Ming chi 2020) Social distancing practices and staying at home have increased the time people spend on social media with the purpose of exchanging and consuming information about completing their routine practices safely. the world has moved toward internet banking with the purpose to continue routine transactions for paying bills, purchasing groceries, and shopping of brands. **(Tiago Oliver 2009)**Cybercrime is a bigger risk now than ever. Illegal activities conducted by cyber fraudsters and criminals using electronic means such as computers, mobiles and other network devices are genus of crimes which are transitional in nature compare to traditional crimes. Cyber criminals use a number of methods depending on their skills set and their goals and objectives. The rapid growth in cybercrimes is the main concern for financial institutions in the 21st century and the need to protect the cyberspace is becoming more critical than ever before.(Muhammed Naeem 2020) E-Banking has become an important factor in the future development of banking industry. Electronic banking or online banking is a service provide by many banks that allow handling of all types of banking business, primarily over the internet by using the information technology and communication. In many developed countries E-banking plays a very vital role due to the fact that it's the cheapest way of providing banking services. Beside this it also facilitated swift movement of funds domestically and across borders.**(Liaqat 2021)** Online banking faces different kind of risks that are specific to conducting sensitive business over the Internet. It is imperative that banks implement strong security approaches that can adequately address, monitor, manage, and control risks and security threats. This paper demonstrates that the online banking may confront operational, security, legal, and reputation risks. The risk management consists of strategic planning, identifying, analysis, monitoring and manage risks.**(Hajeria Fatima 2008)** Internet banking and other modes of e-banking have been a blessing for banking as far as speed, convenience and cost of delivery is concerned, but alongside it has brought many risks. It has also brought about a new orientation to risks and evennew forms of risks. Technology plays a significant part both as source and tool for control of risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures.**(Nein jin 2020)** The new information technology is becoming an important factor in the future development of financial services industry, and especially banking industry. Growing international trading and problems in transferring money have motivated researchers to introduce a new structure. E-banking is such idea. Most of banks are using the Internet as a new distribution channel. This paper presents a through survey of e-banking describing definition, barriers, benefits from the customers', economy, and bank point of views, and main issues and challenges such as risk management and factors responsible for e-banking development.(Virendr Singh 2003) This paper investigates the risk, efficiency and rate of progress in the implementation of electronic commerce (e-commerce) and emerging markets. The results confirm that the US is very advanced in its electronic-banking (e-banking) actuation. There is evidence suggesting that e-banking is driven largely by the prospects of operating costs minimisation and operating revenue maximization.**(Simpson 2022)**

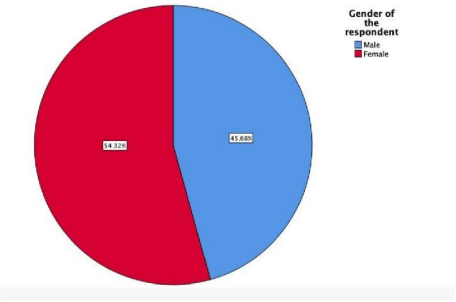
III. RESEARCH METHODOLOGY:

The research method followed in the research is empirical research. Total of 211 samples have been collected through a convenient sampling method. The samples were collected through a questionnaire survey. The sampling frame was taken from Chennai. The sampling data was collected through an online and offline survey. The independent variables are age, gender, place of living and educational qualification (of the respondent). The dependent variables are for which purpose, how often do you use, do you agree with the statement, the most common mode of online transaction. The statistical tool used here to represent the data is pie charts and graphical representation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

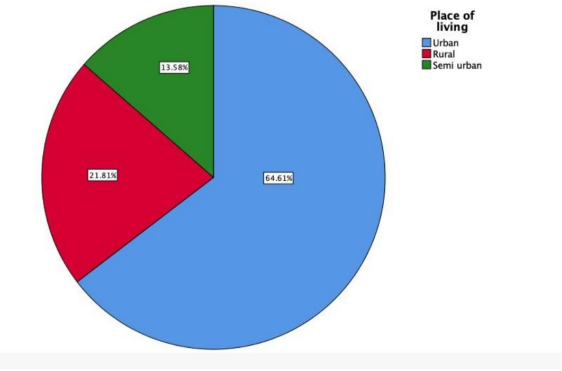
IV. GRAPHICAL REPRESENTATION

FIGURE 1



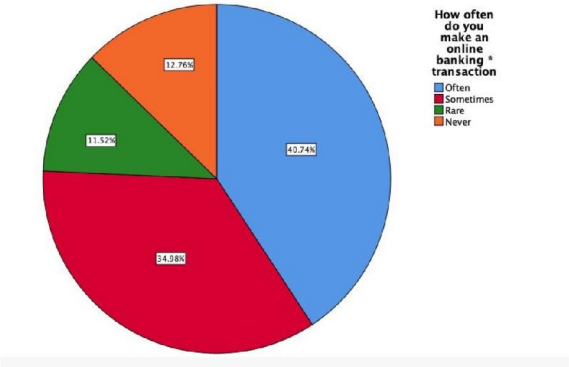
LEGEND: figure 1 represents gender of respondent

FIGURE 2



LEGEND: figure two represents place of living of respondent

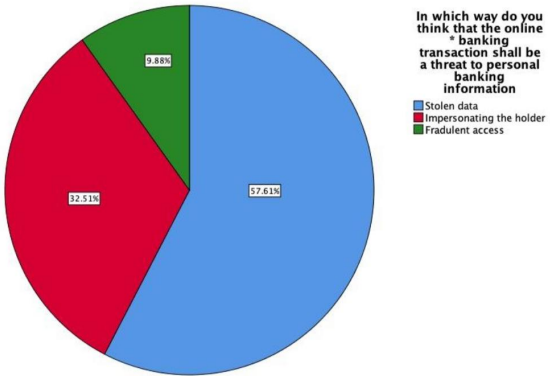
FIGURE 3



LEGEND: figure 3 shall represent. How often do you make an online banking transaction?

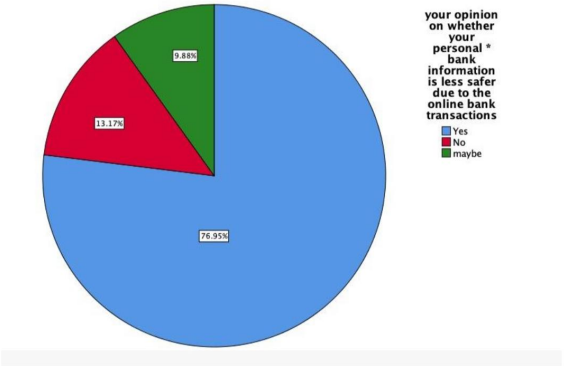
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 4



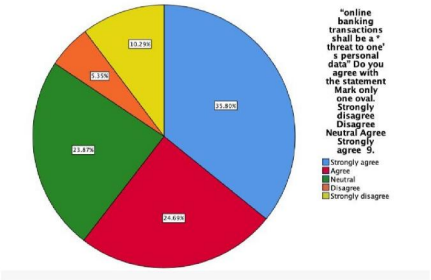
LEGEND: figure 4 represents. In which way do you think that the online banking transaction shall be a threat to personal banking information?

FIGURE 5



LEGEND: figure 5 represent your opinion on whether your real personal bank information is less safer due to the online bank transactions

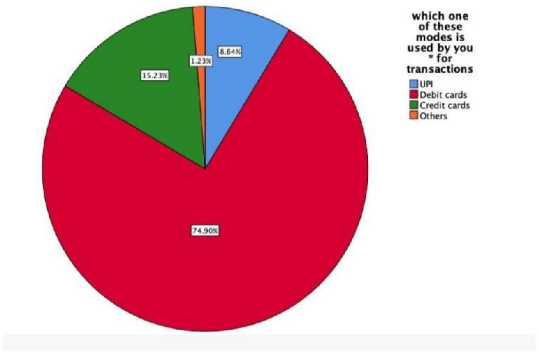
FIGURE 6



LEGEND: figure 6 represents weather, online banking transactions shall be a threat to personal income

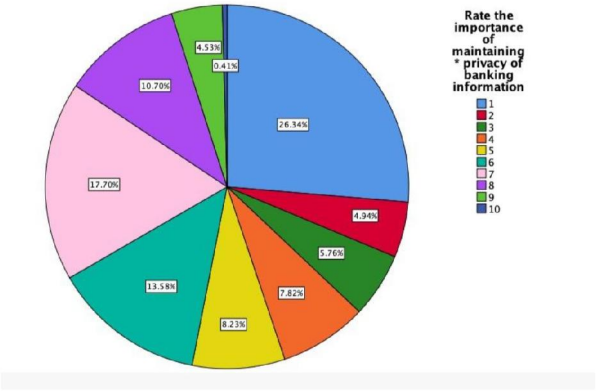
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 7



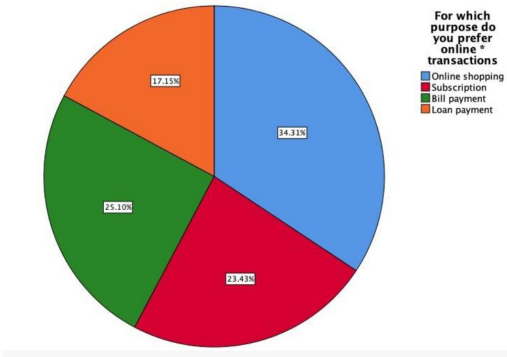
LEGEND: figure 7 represents which one of these modes is used by you or transactions

FIGURE 8



LEGEND: figure 8 represents rate the importance of maintaining privacy of banking Information

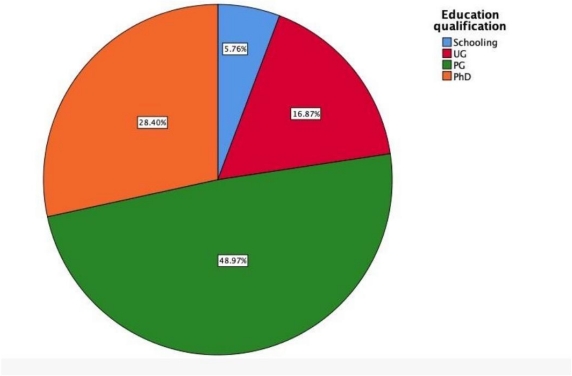
FIGURE 9



LEGEND: Figure nine represent a preference, for which purpose do you prefer online transactions?

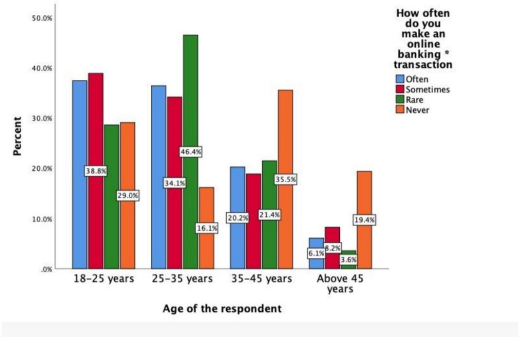
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 10



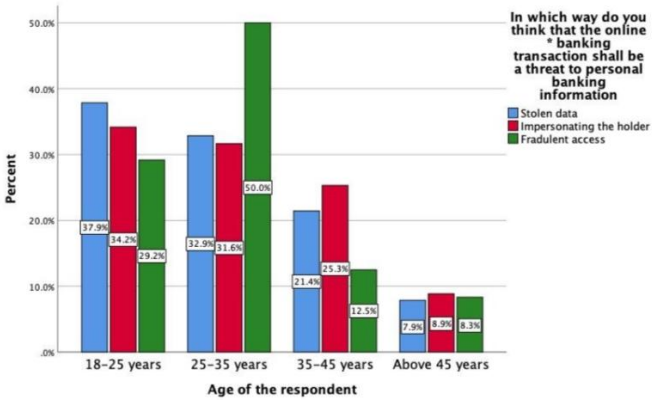
LEGEND: figure 10 shall represent the education College

FIGURE 11



LEGEND: figure 11 represent the age of respondent and how often do you make an online Banking

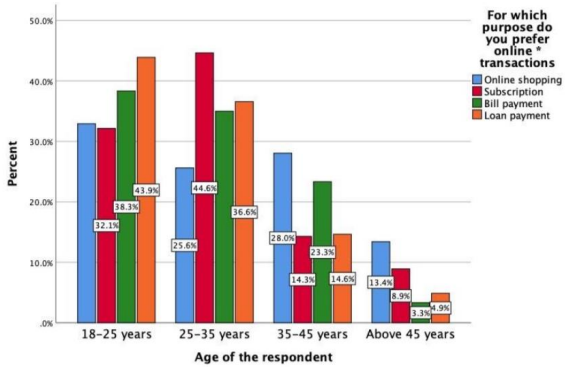
FIGURE 12



LEGEND: figure 12 shall represent the age of respondent and in which way do you think that the online banking transaction shall be at threat to personal information

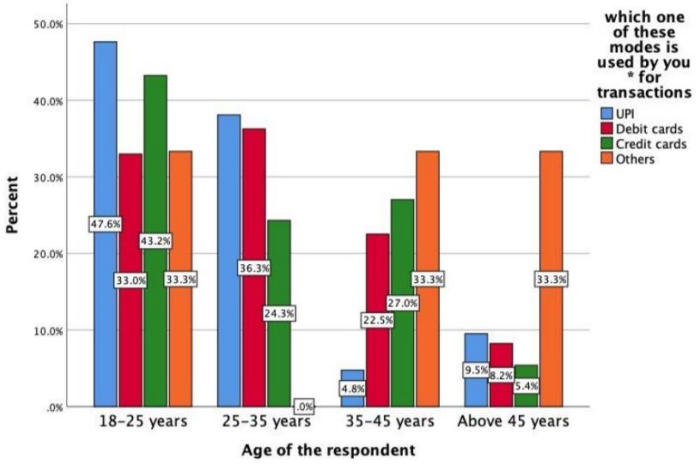
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 13



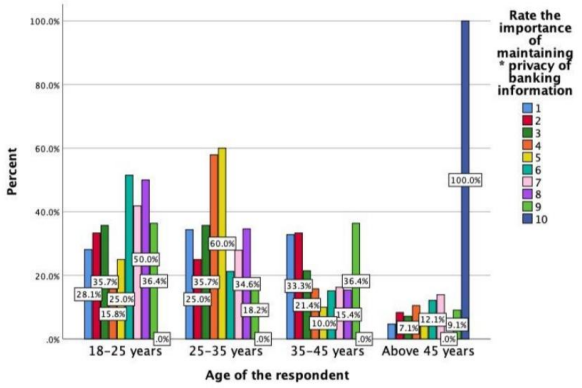
LEGEND: figure 13 shall represent age of respondent and for which purpose do you prefer online banking transaction?

FIGURE 14



LEGEND: figure 14 shall represent age of respondent and which one of these mode is used for transaction.

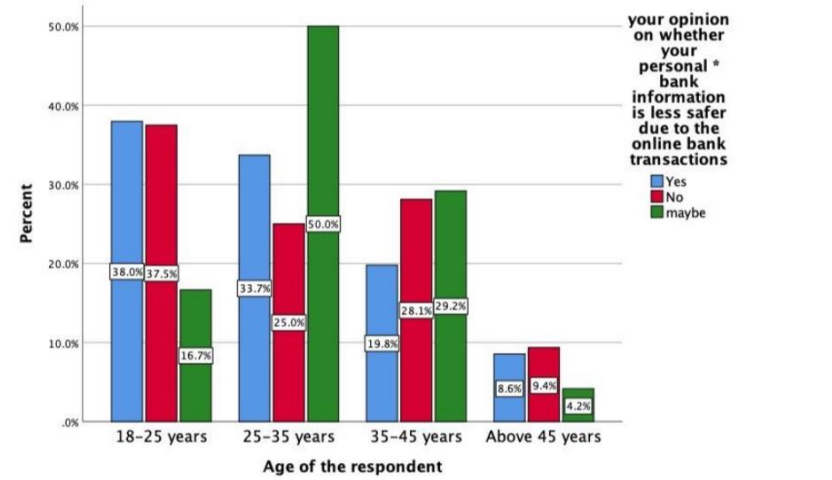
FIGURE 15



LEGEND: figure 15 shall represent age of respondent and read the importance of maintaining banking privacy information

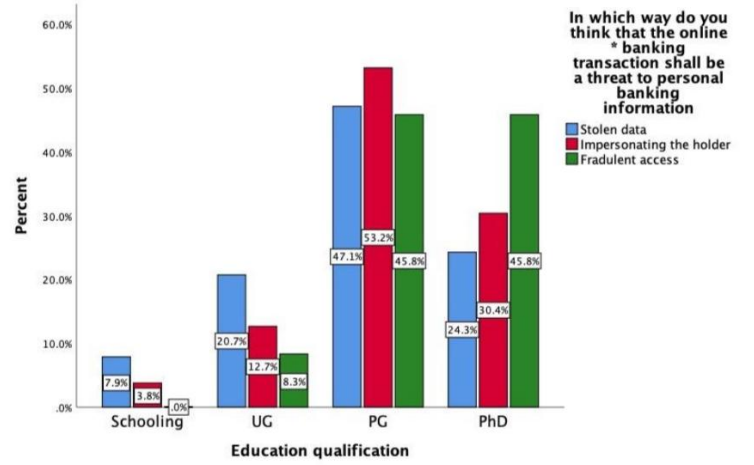
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 16



LEGEND: figure 16 represent age of respondent and your opinion on whether your personal bank information is less safer due to online banking transaction

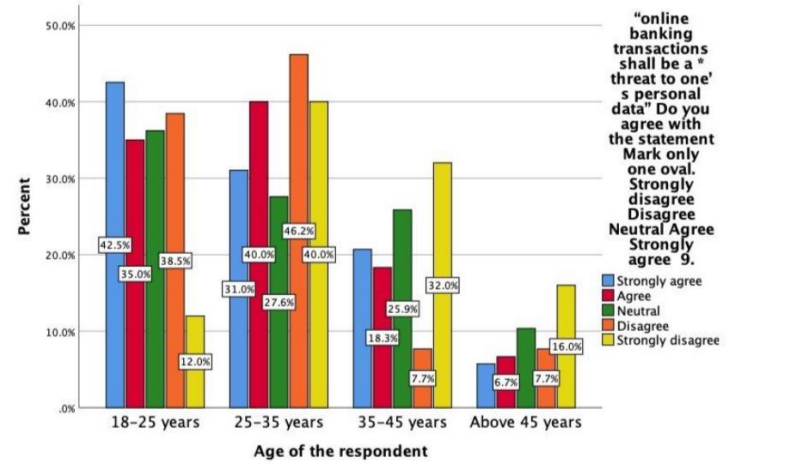
FIGURE 17



LEGEND: figure 17 represent educational qualification and in which way do you think that online banking transaction shall be a threat to personal banking information?

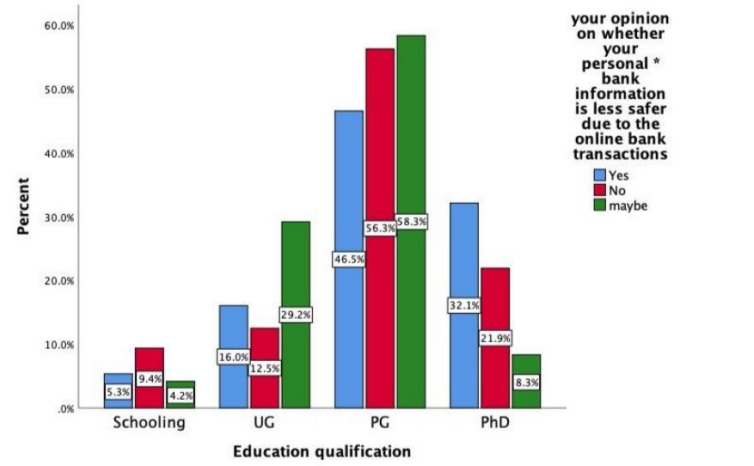
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 18



LEGEND: figure 18 shall represent age of respondent and do you agree with the statement?

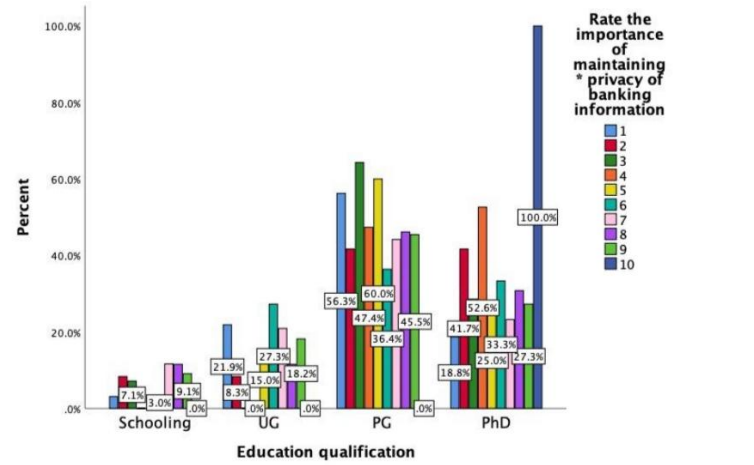
FIGURE 19



LEGEND: figure 19 represent , educational qualification and your opinion on whether your personal bank information is less safer due to the online bank transactions

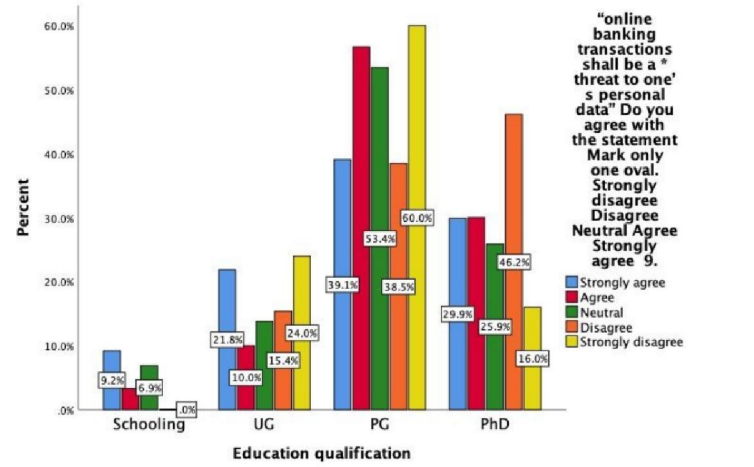
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 20



LEGEND: figure 20 shall represent the educational qualification and read the importance of maintaining privacy of banking information

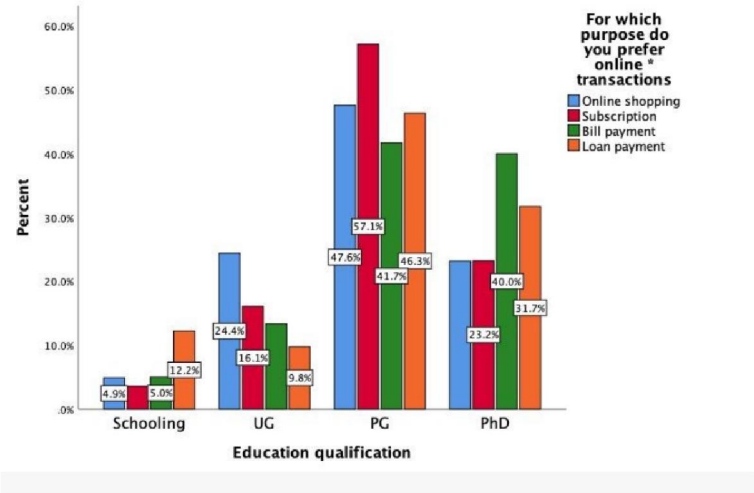
FIGURE 21



LEGEND: figure 21 shall represent educational qualification and do you agree with the Statement?

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

FIGURE 22



LEGEND: figure 22 shall represent educational qualification, and for which purpose do you prefer online transactions

V. RESULTS:

From figure 1 we can analyze that 45.68% are male respondents and 54.32% or female respondents from figure 2 we can analyze that 64.61% Arab and respondents 21.81% or from FIGURE 1 rural ared 13.58% are from semi urban area. From figure 3 we can analyze that 40.74% have said that they often make an online banking transaction, 34.98% have said sometimes 11.52% have said a rare and 12.76% have said never to the question of making an online banking transaction. From figure 4 we can analyze that 57.61% have said stolen data is the most personal information threat analyzed by them while making an online transaction, 32.51% have said impersonating the holder of the account, 9.88% have said fraud and access to the transaction or account banking details is the threat to them. From figure 5 we can analyze that 70 65.95% have said yes to whether their personal bank information is less safe due to the online banking transaction in majority and 13.71% have said no to the same and 9.88% have said maybe to the same statement. From figure 6 we can analyze that the online banking transaction shall be a threat to one's personal data as 35.80% of respondents in majority strongly agree to the statement 24.69% stay neutral to the statement 23.87% agree to the statement 10.29% strongly agree to the statement and 5.35% disagree to the statement. From figure 7 we can analyze that 74.90% have said debit cards are the most common mode used by them for transactions the second most used more easy credit cards and 8.64% have said UPI the rest have said other options. From figure 8 we can analyze the importance of maintaining privacy of banking information. Most of the respondents have rated above the scale of seven which is 79 and 10 the highest percentage shall be one which is 26.34 percentage. From figure 9 we can analyze that the purpose which is most common for online transactionIs for online shopping which is 34.31% and the least is for loan payment which is 17.15% in majority. From figure 10 we can analyze that most of the respondents are from the post graduates which is 48.97% and the least respondents are from schooling which is 5.76 percentage from figure 11 we can analyze that age group of 18 to 25 years have said sometimes which is 18.8%. 25 to 35 years have said a rare 46.4%. Age group of 35 to 45 years have told no which is 35.5 percent. Above 45 years have said never which is 19.4 percent. From figure 12 we can analyze that 18 to 25 years have said stolen data which is 37.9 percentage age-group of 25 to 35 years have said fraudulent access which is 50 percentage is group of 35 to 45 years have said impersonating the holder which is 25.3 percentage above 45 years have said impersonating the holder which is 8.9 percentage. From figure 13 we can analyzethat 18 to 25 years and above 45 years have said loan payment 43.9% and 4.9% respectively. 25 to 35 years have shared online shopping and 35 to 45 years have also said online shopping. From figure 14 we can

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

analyze that 18 to 25 years have said UPI which is 47.6 percent. 25 to 35 years FIGURE 1 have also said UBI which is 36.3 percent. 35 to 45 years have said others which is 33.3percent and above 45 years have also said others which is 33.3 percent. From figure 15 we can analyze that 18 to 25 years and 35 to 45 years have rated the highest importance and 25 to 35 years and above 45 years have given least rating. From figure 16 we can analyze that this group of 18 to 25 years have said yes which is 38.0% in majority where 25 to 35 years and above 35 years have said maybe to the statement that the personal bank information is less safe due to online banking transactions. From figure 16 we can analyze that schooling respondents and Anju graduates have said stolen data as a threat 7.9% 20.7% respectively. P&G have said 53.2% impersonating the holder. From figure 18 we can analyze that the younger generation of the age group 18 to 25 years have strongly agreed to the statement whereas most of the older generation have state neutral to the statement. From figure 21 we can analyze that schooling and undergraduate respondents have strongly agreed, which is 9.2 percentage and 21.8 percentage. From figure 22 we can analyze that schooling respondents have said loan payment whereas others have said Online shopping and majority which is 47.6 percent and 40.2 percent.

VI. DISCUSSION:

From figure 3, we can analyse that most of the respondents have responded that they often make an online banking transaction. From this, we can say that most of the respondents know how to do banking transactions and have done online transactions and payments. From figure 4, we can analyse that, most of the respondents have thought that the stolen data is the threat to the personal banking information. There are other modes through which the personal information of banking transaction can be obtained by a third person but as stolen data is most common, the public might have chosen it in majority. From figure 5, we can analyse that the personal bank information is comparatively less safe due to the online banking transactions. Most of therespondents have said yes as all the details of their personal Bank account and cards are involved and needed for online banking transaction. From figure 6. We can analyse that most of the respondents think that online banking transactions shall be read to the personal data and it is not FIGURE 1 denied as mostly common people were facing the issue. From figure 7, we can analyse that, the common mode of online transaction is by using debit cards, as all the account holders mostly have debit cards. It shall be the most commonly used mode for making online payments and transactions. From figure 8, we can analyse that most of the respondents of different categories have less awareness about maintaining the privacy of banking information. From as of the respondents think that the purpose for which one shall prefer online transaction is online shopping. From figure 15 We can analyse that all the age groups Have knowledge on maintaining the banking information is privacy. From figure 16, we can analyse that most of the younger generation below the age of 35 years have said that their personal banking information is less safe. above the age of 45 years have said no to the statement. From figure 17, we can analyse that most of the schooling undergraduate respondents think that stolen data shall be the threat as it is the most commonly found method to obtain a person's banking information. From figure 19, we can analyse that most of the respondents who were above the education level of schooling, Dhinta Da banking information is comparatively less Safe duty online banking transaction.

VII. LIMITATIONS:

The samples are obtained in the convenient sampling method and the sample size is 211. We can not determine the opinion of people in Chennai with a small sample size. This is a limitation and a disadvantage to the research. We can not collect samples from the entire population of India. This data is also taken from a sample frame of a particular region in Chennai.

VIII. CONCLUSION:

From this research, we can conclude that the respondents respective of their educational qualification or have knowledge about the online banking transaction and how often the transactions were leading to threat of their personal banking information. It is also important to note that the younger generation know the importance of maintaining the privacy of the information and how it might cause a threat to a person if not maintained. Most of the online transactions and payments were found to be either from online shopping or from subscription. We can conclude that there is a rise in

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

online banking transactions and there is a threat to personal information due to online banking which can not be evaded even with utmost care as all private information is necessary.

REFERENCE:

[1]. AEli, Liaqat. "Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC)." The Journal of Developing Areas, vol. 53 no. 1, 2019. Project MUSE, doi:10.1353/jda.2019.0016.

[2]. Testing a model of precautionary online behaviour: The case of online banking, Computers in Human Behavior, Volume 87, 2018, Pages 371-383, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2018.05.010.

[3]. Nie Jin and Ma Fei-Cheng, "Network security risks in online banking," Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005., 2005, pp. 1229-1234, doi: 10.1109/WCNM.2005.1544265.

[4]. Kinana Jammoul, Habin Lee, Jisun Kim, Moongil Yoon, Uthayasankar Sivarajah. (2022) Antecedents and Moderators of Promotion Messages for Trust in Mobile Banking Services: An Elaboration Likelihood Model Perspective. Information Systems Management 0:0, pages 1-21.

[5]. Kesharwani, A. and Singh Bisht, S. (2012), "The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model", International Journal of Bank Marketing, Vol. 30 No. 4, pp. 303-322. https://doi.org/ 10.1108/02652321211236923

[6]. Guriting, P. and Oly Ndubisi, N. (2006), "Borneo online banking: evaluating customer perceptions and behavioural intention", Management Research News, Vol. 29 No. 1/2, pp. 6-15. https://doi.org/10.1108/01409170610645402

[7]. K. Edge, R. Raines, M. Grimaila, R. Baldwin, R. Bennington and C. Reuter, "The Use of Attack and Protection Trees to Analyze Security for an Online Banking System," 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007, pp. 144b-144b, doi: 10.1109/HICSS.2007.558.8.

[8]. A proposed framework for accelerating technology trajectories in agriculture: a case study in ChinaBeth CLARK et al., Frontiers of Agricultural Science and Engineering,

[9]. Lichtenstein & Williamson: Consumer Adoption of Internet Banking UNDERSTANDING CONSUMER ADOPTION OF INTERNET BANKING: AN INTERPRETIVE STUDY IN

[10]. Hanafizadeh, P., Khedmatgozar, H.R. The mediating role of the dimensions of the perceived risk in the effect of customers' awareness on the adoption of Internet banking in Iran. Electron Commer Res 12, 151–175 (2012). https://doi.org/ 10.1007/s10660-012-9090-z

[11]. Impact of e-banking on traditional banking services Shilpan Dineshkumar Vyas arXiv preprint arXiv:1209.2368, 2012

[12]. A logit analysis of electronic banking in New Zealand Christopher Gan, Mike Clemes, Visit Limsombunchai, Amy Weng International Journal of Bank Marketing, 2006

[13]. Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit Ming-Chi LeeElectronic commerce research and applications 8 (3), 130-141, 2009

[14]. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application Carolina Martins, Tiago Oliveira, Aleš Popovič International journal of information management 34 (1), 1-13, 201415.

[15]. The role of social media in internet banking transition during COVID-19 pandemic: Using multiple methods and sources in qualitative research Muhammad Naeem, Wilson Ozuem Journal of Retailing and Consumer Services 60, 102483, 2021

[16]. Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC) Liaqat Ali The Journal of Developing Areas 53 (1), 2019

[17]. E-banking: Benefits and issues Hajera Fatima Khan American Research Journal of Business and Management 3 (1), 1-7, 2017

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

[18]. Network security risks in online banking Nie Jin, MA Fei-Cheng Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005. 2, 1229-1234, 2005

[19]. Risks in e-banking and their management Virender Singh Solanki International Journal of Marketing, Financial Services & Management Research 1 (9), 164-178, 2012

[20]. The impact of the Internet in banking: observations and evidence from developed and emerging markets John Simpson Telematics and Informatics 19 (4), 315-330, 2002