Impact of Cybersecurity Awareness on user Behaviour in Digital Banking: A Study on Risk Perception, Preparedness and Financial Implications

Adapa Shirisha[1], Dr. Yesubabu Konga[2]

[1]Post-Graduate Student (MBA), School of Management Studies, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India

[2]Assistant Professor, School of Management Studies, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad,

*Corresponding Author: shirishaadapa04@gmail.com

How to Cite this Article:

Shirisha, A. (2026). Impact of Cybersecurity Awareness on user Behaviour in Digital Banking: A Study on Risk Perception, Preparedness and Financial Implications. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.657

https://doi.org/10.55041/ijcope.v2i4.657

ABSTRACT

The rapid growth of digital banking provides consumers with a high level of access and convenience to their banking services. Unfortunately, it has made them more vulnerable to various types of computer crime such as phishing, OTP fraud and data breaches, which create a real threat to their financial safety and security. This research aims to demonstrate the ways in which awareness about cybersecurity impacts the behaviour of customers who use digital banking. In particular, it examines the relationship between awareness (of cybersecurity), perceived risk, preparedness, the use of protective measures (i.e. protects against potential cybercrimes), and financial impact. A descriptive, analytical (quantitative) research design was chosen to conduct this study. Primary data collection involved 150 participants (users of digital banking) who completed an online survey. According to SPSS, three types of statistical analysis were performed on the data: Independent Samples t-tests, One-way ANOVAs, and Simple and Multiple Regression. The outcomes show there is no significant difference in awareness of cybersecurity based on gender; however, significant differences were found by age and educational level Additionally, cybersecurity awareness was found to be significantly and positively associated with perceived risk and the uptake of protective strategies. The results also showed that while both preparedness (by itself) and awareness affect financial outcomes, the effects of preparedness are substantially greater than the effects of awareness alone (in isolation). The significance of blending awareness training and practical instruction on preparation for using banking technologies is demonstrated by these results; if individuals were better prepared for the possibility of computer crime, they would be less likely to experience financial loss.

Keywords: *Cybersecurity Awareness, Digital Banking, User Behaviour, Risk Perception, Preparedness, Financial Implications*

I. INTRODUCTION

Over the last ten years the financial services industry in India has changed dramatically due to new technology and increased use of the internet. Digital banking has changed how people conduct day to day financial transactions. Digital banking includes mobile banking, internet banking, UPI systems, and digital wallets. Government-sponsored programs and innovative regulations have helped speed up the transition to digital banking, providing millions of new customers access to the digital economy and cashless transactions have become an everyday occurrence. While users enjoy the benefits of digital banking, they also create new and greater risk for cybercrime. Cybercriminals have become more sophisticated and there is a growing number of threats including phishing attacks, OTP scams, malware, ransomware, and identity theft, which have become more frequent since the introduction of digital banking. Financial institutions in India appear to be the hardest hit by cybercrime and have experienced significantly higher rates of cyber incidents than the international average. The impact on financial losses and customer trust caused by these attacks demonstrates that adequate security infrastructure and a well-informed customer base are necessary components needed to increase the cybersecurity of digital banking.

The weakest point of cybersecurity consistently identified in research is the human user. No matter how sophisticated the technical solutions are, users who do not have the ability or knowledge to identify threats or protect themselves from them or respond correctly to incidents will weaken those technical solutions. For this reason, the development of user awareness must be a key aspect of all serious efforts to secure the digital banking space. Nonetheless, user awareness alone is insufficient: it must result in a changing of users' behaviours and a moving toward actual preparations if there is to be genuine reductions in financial risk. The purpose of this study, therefore, is to investigate the impact of cybersecurity awareness on risk perception and preparedness, as well as on the adoption of protective behaviours among users of digital banking in Hyderabad, Telangana. The study will also examine the combined influences of user awareness and preparation regarding their financial consequences, such as losses experienced and security-related expenses. This research will extend the body of literature regarding the behaviours associated with cybersecurity in emerging digital economies to provide useful information to banks, regulators and policymakers who are trying to develop better user education programs.

II. LITERATURE REVIEW

Recently, there has been a sharp rise in the academic interest surrounding the relationship of cybersecurity awareness with user behaviours related to the use of digital banks. With the increased need to ensure that online banking customers feel secured during an online financial transaction, researchers have begun to spend more time exploring the various issues surrounding user behaviour regarding their understanding of cybersecurity.

Kee et al. (2025) investigated the behavioural determinants of online banking use in Malaysia. They found that individuals' behavioural intention to use online banking for financial transactions was significantly influenced by their perceived risk, perceived ease of use, perceived usefulness, and trust. These researchers concluded that the design of online banking security systems had to be protective of user privacy and operationally support the user experience, as a complex system would potentially reduce user vigilance.

Nagari and Raharja's (2025) study focused on the digital banking users in Salatiga, Indonesia, and they found that knowledge about cybersecurity had a significantly greater direct effect on the safe use of a digital bank than just having awareness of cybersecurity issues. Their results challenged the assumption that awareness of the issues related to cybersecurity would necessarily result in users employing safe behaviours when using a digital bank. Based on their work, the authors strongly recommended that banks provide opportunities for their customers to develop a deep understanding of cybersecurity issues rather than just providing information over-and-over.

Hakimi et al. (2025) studied how AI-based risk communication tools were used to inform e-banking customers about potential cybersecurity threats. Their study demonstrated a substantial gap between customer awareness of cybersecurity issues and safe behaviours in response to these issues. The authors also found that younger respondents had greater levels of awareness and felt a greater degree of trust in using AI-based technology to detect and prevent fraud. The authors recommended developing specific educational strategy for different age groups for educating customers about cybersecurity awareness.

Bhoomika (2025) completed a survey of bank customers in India, and found that there was a considerable gap between respondents' levels of understanding of the privacy policies of banks, and their actual trust in banks regarding data collection and storage. Furthermore, younger customers and those who were more technically savvy had significantly

higher expectations for transparency from their bank than their older counterparts, indicating that enhanced communication strategies by financial institutions are required.

Fatma et al. (2025) assessed the level of awareness about cybersecurity amongst banking customers, by evaluating a sample of urban, semi-urban, and rural customers in India, and utilizing correlation and factor analyses. The researchers concluded that strong relationships exist between respondents' level of knowledge about cybersecurity and their level of trust in online banking platforms. Furthermore, they found that many respondents did not possess a basic knowledge about safe banking practices (e.g., using public Wi-Fi and fraud reporting).

Shah et al. (2024) did a study of university students in Pakistan to determine the effect of cybersecurity awareness on risk perception and preparedness to take precautions when engaging in online activities. The researchers discovered that as respondents' awareness of cybersecurity increased, so did the extent to which they used secure practices (e.g., password management and safe online activity), clearly illustrating not only the behavioural impact of cybersecurity awareness programmes but also the link between participants' level of awareness and the probability that they will implement secure practices.

III. METHODOLOGY

This study has identified several limitations in the existing research literature and will attempt to resolve them. There are two main areas in which previous research has been limited: the individual constructs or variables that have been previously studied individually, and the financial considerations of cybersecurity behaviours of individuals as opposed to financial vulnerability of individuals due solely to their level of awareness regarding cybersecurity. There is also an absence of context-specific evaluations of Digital Banking Users within India, particularly in Telangana due to local cultures, technological capabilities, and levels of digital literacy shaping cybersecurity behaviours. Additionally, while the distinction of awareness (information) versus preparedness (behaviour) has not been explicitly evaluated, the two constructs have significant implications for the implementation of proper and effective education programs to promote better cybersecurity behaviours. By employing an overarching theoretical model that embraces all of these disparities from the current body of literature through the exploration of a single study, hopes to determine the relationship between cybersecurity awareness, risk perception, protective behaviour, preparedness, and financial impact to facilitate stronger programmes.

IV. RESULTS AND DISCUSSION

1. To assess the level of cybersecurity awareness among digital banking users.

2. To examine how users perceive potential risks associated with using digital banking services.

3. To evaluate the extent to which users adopt protective strategies to safeguard their digital financial activities.

4. To investigate how cybersecurity awareness and preparedness affect financial implications.

The following null hypotheses were formulated for testing:

H_{01}: There is no significant difference in cybersecurity awareness between male and female digital banking users.

H_{02}: There is no significant difference in cybersecurity awareness among users of different age groups.

H_{03}: There is no significant difference in cybersecurity awareness among users with different educational qualifications.

H_{04}: There is no significant relationship between cybersecurity awareness and risk perception regarding digital banking services.

H_{05}: There is no significant relationship between cybersecurity awareness and the adoption of protective strategies in digital banking.

H_{06}: Cybersecurity awareness and preparedness do not significantly affect financial implications.

Research Design

The research design consists of two components: Descriptive -which provides information on the current state of cybersecurity awareness, risk perception, preparedness, financial impact to users of digital banking. Analytical - which examines how those variable types relate to each other using appropriate inferential statistical procedures.

Data Collection

Digital banking users were surveyed for primary data via structured questionnaire. The questionnaire consisted of five-point Likert Scale responses from strongly disagree through to strongly agree. Four main areas of study: cybersecurity awareness, risk perception, being prepared before an event, and financial impacts and how they are used relative to their digital banking platforms.

Sampling

To obtain participants for this research project, a random sampling approach was employed to select individuals currently using or involved in using Digital Banking products/services; therefore, a total of 150 individuals were included in the sample group. Before conducting the complete data collection phase, the researchers also performed a pilot study regarding the questionnaire to test its validity as well as reliability, using the pilot results to make any needed changes/adjustments.

Data Analysis

The collected data were analyzed with SPSS. The statistical methods used in this analysis were descriptive statistics (mean, standard deviation, skewness and kurtosis), independent t-tests, one-way ANOVA with Tukey HSD post-hoc comparisons, simple linear regression and multiple linear regression.

Scope and Limitations

This research specifically looks at personal users of digital banks in Hyderabad, Telangana. It is not addressing the infrastructure associated with technology used for providing secure banking. The population for this study is limited geographically and by sample size. Self-reported responses may present response bias. Cyber threats occur in an ever-changing environment, 'the findings may reflect the data collection time and are not representative of future trends of cyber threat activity

Demographic Profile of Respondents

There are an equal number of men (75) and women (75) in the sample of 150 as well as there was a balance of responses across members of each gender (50% men, 50% women). The age group that was most represented among those responding to the survey were individuals between the ages of 21-30 (n=90; 60%). The next two highest numbers of respondents were both for those between the ages of 41-50 and those above the age of 50 (n=16 for both; 11%). The next highest percentage of respondents was for those below the age of 20 (n=15; 10%) and for those between the ages of 31-40 (n=14; 9%).

Educationally, the majority of those responding had obtained their education at the postgraduate level (n=66; 44%) or at the undergraduate level (n=59; 39%). The number of individuals that have completed a Doctorate was 10% and those with a high school diploma and no further education made up 7%. In regard to occupation, the largest number of respondents reported being an employee (43%), with students being the next largest group (39%), self employed/business owners came in at 16%, and other occupations made up the remaining 3%.51% of the total sample (n=91) of respondents reported an income in the below ₹50,000 per month range which is due primarily to the student and early-career employee population represented in the sample.

Table 1: Distribution of Respondents by Gender

Gender	Frequency	Percentage (%)
Female	75	50
Male	75	50
Total	150	100

Table2: Distribution of Respondents by Age Group

Age Category	Frequency	Percentage (%)
Below 20 years	15	10
21-30 years	90	60
31-40 years	13	9
41-50 years	16	11

Above 50 years	16	11
Total	150	100

Digital Banking Platform Usage

The descriptive analysis of the frequency of use for the different platforms used for digital banking shows that UPI applications (mean = 4.55, SD = 0.887) are the most common form of digital bank. Both the median and mode scores for UPI applications are five. This indicates that UPI is an established part of daily payment behaviour within India. In terms of average usage, mobile banking applications (mean = 3.23, SD = 1.313) were used at a slow-to-moderate rate of usage; digital wallets (mean = 3.15, SD = 1.453) generally had a wide variety of different types and methods of usage; whereas the average for internet banking websites (mean = 2.93; SD = 1.168) indicates that internet banking is generally considered less convenient than banking through a mobile or digital application.

Table 3: Descriptive Statistics for Frequency of Usage of Digital banking Platforms

Statistic	**Internet Banking Websites**	**Mobile Banking App**	**UPI Apps**	**Digital Wallets**
Mean	2.93	3.23	4.55	3.15
Std. Deviation	1.168	1.313	0.887	1.453
Median	3.00	3.00	5.00	3.00
Mode	4	4	5	5

Cybersecurity Awareness

Overall, participants displayed an intermediate range to slightly above average level of awareness about Cybersecurity. The greatest percentage of indicants belong within the area of strong and/or unique password awareness, producing a mean score of 4.17 (SD = 1.14), with a median of 5 and mode of 5. Participants indicated a lower degree of awareness regarding phishing attacks and malware, as reflected by a mean of 3.63 (SD = 1.15) and 3.64 (SD = 1.166) respectively; while the least amount of variability existed when participants provided their means for consistently updating applications and devices associated to banking was reflected in a mean of 3.61 (SD = 1.215) therefore indicating that this manner is not continuously adhered to by all participants. All four variables were negatively skewed, confirming a greater tendency to provide above average ratings in respect to awareness level when completing each item**.**

Risk Perception

Most respondents perceived digital banking as being of moderate or high risk. All but one of the responses by participants (the one regarding how vulnerable someone is to being victimized by cyberattacks) fell in the upper (i.e., 4 - 5) range of the scale, indicating the presence of widespread anxiety with respect to data integrity. The responses that pertained to concerns about potential loss/theft of personal/financial information online were the highest of the group, with a mean response of 3.79 (SD = 1.127) and a mode of 5. Respondents also indicated that they considered digital banking to pose a greater likelihood of risk of loss/theft than traditional banking with a mean response of 3.74 (SD = 1.132). Similarly, respondents also felt the likelihood of falling victim to cyber fraud as a result of using digital banking was comparatively greater than using traditional banking (mean 3.73, SD = 1.023). While indicating that data integrity is a potential issue and concern was the response related to vulnerability to being victimized through a cyberattack during electronic transactions; however this particular response had the lowest of the four means at 3.69. Overall, all four responses reflected a significant negative skew, between .514 and .597, indicating greater than expected concentration of the responses in the upper end of the scale.

Digital Banking Usage Behaviour

All four responses to the digital banking usage behavior measurements show means greater than 4.00, with modes of 5, representing an increased level of digital banking use and an increase in the amount of digital banking service available to users. The increased use of digital banking in general was the most significant at 4.27 (SD = 1.034) with a median of 5, so there has clearly been a shift in user behavior over time. The means for the frequency of use of digital banking and preference to use digital banking rather than visit a physical branch were also significant at 4.04 and 4.01, respectively. The strong negative skewness on the entire digital banking usage measurement supports that the digital banking usage measurements were all skewed to a high volume of responses.

Preparedness

On average, the respondents of this research reported a moderate level of preparedness to deal with incidents arising from cyber security in online banking. They demonstrated moderate levels of preparedness with an overall mean score of 3.66 (SD = 1.284) out of 5 currently reported for the item belief that they are well prepared to respond to cyber threats. There was substantial variance across the sample with some respondents feeling unprepared due to low scores on this item. The respondents had a mean score of 3.61 (SD = 1.180) for the knowledge of bank security options available to them and a mean score of 3.57 (SD = 1.166) for knowing what they should do when banking credentials are compromised. The respondents' weakest level of preparedness was their confidence in dealing with suspicious bank transactions or incidents in real time, which had the lowest mean score of 3.33 (SD = 1.168), with a median score only equalling 3. This indicates that there is a disconnect between the amount of information one has and their level of confidence to actually take action when confronted with an incident.

Financial Implications

The average level of financial worry related to cyber security was moderate. The biggest worry for those surveyed was about the potential for financial loss as a result of cyber attacks (related to digital banking) this received a mean value of 3.61 (SD = 1.086) (and a median and modal response of 4). Reported incidents of financial loss due to personal experiences or those developing through acquaintances was correlated with a mean of 3.53 (SD = 1.235), suggesting that those outside of the sample are frequently already aware of the risks associated with cyber crime either first-hand or through others. The mean for the perceived cost of protecting digital banking accounts was 3.51 (SD = 1.008). The lowest average for reported expenditures on security tools or measures to help protect accounts was 3.32 (SD = 1.287), indicating that while there is a level of concern about financial loss due to cyber attacks, there is not a uniform level of investment in security technology among users.

Hypothesis Testing

H_{01}: Gender and Cybersecurity Awareness (Independent Samples T-Test)

The independent samples t-test results suggest a difference in cyber awareness based on male and female grouping in digital banking users. Women participants on average reported slightly greater awareness scores (M = 3.8767 and SD = 0.881) than men (M = 3.6500 and SD = 1.061). Additionally, Levene's Test indicated no violation of the equality of variance assumption, with a p-value of .068 (which exceeds the.05 alpha level). Finally, the t-test results had a p-value of .157 (which is above the accepted p-value level of .05) therefore it can be concluded there is no statistically or significantly different cyber awareness between genders in digital banking users and that they both have substantially similar levels of awareness.

Table 4: Group Statistics and T-Test Results — Gender and Cybersecurity Awareness

Group	N	Mean	Std. Dev	t	Sig. (2-tailed)
Female	75	3.8767	0.881	1.423	0.157
Male	75	3.6500	1.061	_	_

H_{02}:Age Group and Cybersecurity Awareness (One-Way ANOVA)

A one-way ANOVA was applied in the analysis of how much the degree of knowledge about cyber security is different between the different ages of participants. The mean and standard deviation values show that the group of people in the age range of 21 - 30 years of age had the largest amount of knowledge about cyber security (mean = 3.9611; standard

deviation = 0.916). The two following closest groups of respondents were: people ages 0 - 19 (mean = 3.9500) and people ages 31 - 40 years of age (mean = 3.8269). As the age of the participants are older than 41 years, their score on knowledge of cyber security declines significantly with the lowest level (2.9688; SD = 1.072) being the group of above 50 years. Post hoc comparisons were calculated using Tukey's HSD to confirm that there are statistically different levels of knowledge between certain age groups. There were statistically significant differences ($p < 0.01$) between the 21 - 30 years and above 50 years age groups, the 21 - 30 years and 41 - 50 years age groups ($p < 0.05$), and between below 19 years and above 50 year. However, there were no statistically significant differences in knowledge of cyber security for all respondents aged under 40 years. The null hypothesis was rejected; it is concluded that there is a significant relationship between age and knowledge about cyber security, as the younger the participant is, the higher their knowledge about cyber security.

Table 5: Descriptive Statistics — Cybersecurity Awareness across Age Groups

Age Group	N	Mean	Std. Dev	Std. Error	Min	Max
Below 20 years	15	3.9500	0.621	0.160	2.75	5.00
21-30 years	90	3.9611	0.916	0.097	1.00	5.00
31-40 years	13	3.8269	1.033	0.286	2.25	5.00
41-50 years	16	3.2188	0.953	0.238	2.00	5.00
Above 50 years	16	2.9688	1.072	0.268	1.00	4.50
Total	150	3.7633	0.979	0.080	1.00	5.00

H_{03}: Educational Qualification and Cybersecurity Awareness (One-Way ANOVA)

The Games-Howell post hoc test was performed to locate where the differences were located between each educational group after a significant ANOVA identified a difference within the groups as depicted by ($F = 4.232$, $p = 0.007$). The Games-Howell test is useful in this case because it provides appropriate statistical results despite size and variance inequality across groups and categories. The High School group and Post Graduate Group comparison indicated the greatest difference with a p-value equal to $p = 0.030$ suggesting that individuals possessing only a High School education were not nearly as aware of cybersecurity as compared to individuals obtaining a Post Graduate education. The High School Group and Doctorate Group had a p-value equal to $p = 0.057$ which is just shy of statistical significance; however, it does represent a sizeable gap in a practical sense. Comparisons of the three post-secondary training groups didn't produce any statistically significant differences among themselves although their mean scores were all similarly rated suggesting that their educational levels were not significantly impacting their awareness of online banking safety. In summary this data suggests very strongly that there is a cut-off point in being aware of online banking safety at a particular educational level regardless of whether the educational level was awarded by a master's or Ph.D.

Table 6: Descriptive Statistics — Cybersecurity Awareness across Educational Levels

Educational Level	N	Mean	Std.Dev.	Std. Error
High School	10	2.8250	1.014	0.321
Undergraduate	59	3.6949	1.074	0.140
Postgraduate	66	3.9470	0.871	0.107

Doctorate	15	3.8500	0.646	0.167
Total	150	3.7633	0.979	0.080

H_{04} :Cybersecurity Awareness and Risk Perception (Simple Regression)

An analysis was completed to understand how well cybersecurity knowledge affects how a person perceives threat to their data. Descriptive statistics showed that perceived threat was found to have an average rating of 4.0983 (SD=0.906) and cybersecurity knowledge was found to have an average rating of 3.7633 (SD=0.979). Correlational analysis showed there was a correlation (R) of 0.681 with an R-squared value of 0.464 showing the amount of variance of perceived risk that can be predicted by the knowledge of cybersecurity awareness was 46.4%. There was a positive regression coefficient (B=0.631, β=0.681, p=0.000) which indicates that increasing one's level of cybersecurity knowledge will result in an increased level of the perceived risk in digital banking. As such, the null hypothesis has been rejected for this analysis.

Table 7: Model Summary and Regression Coefficients — Cybersecurity Awareness and Perceived Risk

Predictor	**R**	**R^2**	**B**	**β**	**Sig.**
Cybersecurity Awareness → Perceived Risk	0.681	0.464	0.631	0.681	0.000

H_{05}: Cybersecurity Awareness and Adoption of Protective Strategies (Simple Regression)

A simple regression analysis was conducted to explore how Cybersecurity Awareness impacted the likelihood to adopt Protective Strategies. The mean Protective Strategies adoption score across the sample was 3.9550 (SD = 0.913). The model developed a correlation coefficient of 0.775 and R^2 of 0.601, indicating that 60.1% of the variance in Protective Strategies adoption can be accounted for by Cybersecurity Awareness — this is the strongest predictor found in this study. A positive regression coefficient was calculated (B = 0.723, β = 0.775, p = 0.000), indicating that individuals with higher levels of Cybersecurity Awareness will significantly increase their likelihood of adopting security measures within the context of digital banking. The null hypothesis is rejected.

Table 8: Model Summary and Regression Coefficients — Cybersecurity Awareness and Protective Strategies Adoption

Predictor	**R**	**R^2**	**B**	**β**	**Sig.**
Cybersecurity Awareness → Protective Strategies	0.775	0.601	0.723	0.775	0.000

H_{06}: Cybersecurity Awareness, Preparedness, and Financial Implications (Multiple Regression)

The statistical analysis of multiple regression showed that there is a positive relationship between cybersecurity awareness and preparedness (independent variables) and the financial implications of cyber threats (dependent variable). The results indicated that both of the predictor variables explain 31.8% of the variance in financial implications (R2 =.318). A further analysis of individual coefficients showed that preparedness positively influenced financial implications (β = 0.589, p = 0.000). This indicates that users that are more prepared to respond to cyber-attacks are more likely to manage and mitigate financial risks associated with a cyber-attack. On the other hand, the findings of this study suggest that users who have higher levels of cybersecurity awareness do not demonstrate positive financial outcomes related to cyber threats (β = −0.043, p = 0.621). As a result, the null hypothesis is rejected because preparedness is a significant predictor of financial outcomes; however, awareness by itself does not predict financial outcomes.

Table 9: Regression Coefficients — Cybersecurity Awareness and Preparedness on Financial Implications

Predictor	**R**	**R^2**	**B**	**β**	**Sig.**

Model (R = 0.564, R^2 = 0.318)	—	—	—	—	—
Cybersecurity Awareness	—	—	−0.035	−0.043	0.621
Preparedness	—	—	0.486	0.589	0.000***

Table 10: Summary of Hypothesis Testing Results

H_0	**Hypothesis**	**Test Used**	**Result**
H_{01}	No significant difference in awareness between genders	Independent t-test	Accepted
H_{02}	No significant difference in awareness across age groups	One-way ANOVA	Rejected
H_{03}	No significant difference in awareness across education levels	One-way ANOVA	Rejected
H_{04}	No significant relationship between awareness and risk perception	Regression	Rejected
H_{05}	No significant relationship between awareness and protective strategies	Regression	Rejected
H_{06}	Awareness and preparedness do not affect financial implications	Multiple Regression	Rejected

V. CONCLUSION

The data demonstrates that there is no significant difference in the levels of cybersecurity awareness between male and female users of a digital bank; however, female participants exhibited higher mean scores. Age and education were shown to be statistically significant correlates of user cybersecurity awareness such that there was a strong level of awareness found among younger participants and those with a higher education level, suggesting that older demographics and participants with lower levels of education represent important opportunities for targeted awareness campaigns. A strong and positive correlation was shown between cybersecurity awareness and risk perception (R^2 = 0.464) and a strong, and positive correlation was shown between cybersecurity awareness and adoption of protective strategies (R^2 = 0.601). The latter of these results, identifying a strong relationship, indicates that users informed about cybersecurity as a result of awareness engage in actions that indicate their understanding and/or adherence to engaging in cybersecurity protective measures and banks/regulators can facilitate the behavioural chain through effective educational campaigns.

The results of these findings provide clear expectations for financial institutions, regulators, and policymakers. Financial institutions (i.e., banks) need to go beyond providing general awareness messages and should develop interventions that help to build user preparedness to respond appropriately to actual cyber incidents. Additionally, awareness expansion programs should be created that take into account user demographics; older adults and adults with lower educational attainment are of particular importance. Providing digital literacy programs in conjunction with full transparency with users about the bank's security measures will assist in closing the current gap between cyber awareness and cyber preparedness that many individuals experience which ultimately results in a high level of financial risk for those users.

There are several limitations associated with this research that should be considered in discussion of the results. First, the sample was taken from a specific location and may not accurately reflect the full range of digital banking customers

throughout India or any developing countries. Second, although 150 subjects (the total number of subjects) is a reasonable size for the analyses; this limits my ability to generalise the results. Finally, self-reported surveys can be subject to social desirability bias which means that the subjects (participants) may be overstating their level of awareness and/or preparedness. To improve future research, researchers could employ bigger and/or more geographically diverse samples; use qualitative approaches to better understand participants' experiences of cybercrimes; and look at the longitudinal effects of specific education or training interventions on financial outcomes. Comparative studies among demographic groups and/or different institutions will further enhance the understanding of how cyber-security behaviours develop and can be influenced through digital banking.

REFERENCES

[1] Kee, D. M. H., Lim, H. N., Lim, B. C., Lim, H. Y., Lim, S. E., Lim, W. Y., & A. J. (2025). Click with care: Understanding cybersecurity awareness in digital financial transactions in Malaysia. International Journal of Tourism and Hospitality in Asia Pacific, 8(2), 179–197.

[2] Nagari, S. F., & Raharja, S. (2025). Cyber security awareness, knowledge and behavior of digital banking users in Salatiga. Asia Pacific Fraud Journal, 10(1), 15–29.

[3] Gopalan, P., & Sathya Devi, D. (2025). The impact of cybersecurity awareness on customers' trust and adoption of internet banking in Palakkad District, Kerala. International Journal of Innovative Research in Technology, 11(12), 6418–6426.

[4] Hakimi, M., Kohistani, A. J., Sahnosh, F. A., Samadzai, A. W., & Enayat, W. (2025). Enhancing customer awareness of cybersecurity threats in e-banking: A study on the role of AI-based risk communication tools. Journal of Management and Business Studies, 10(2), 45–58.

[5] Adejumo, A. P., & Ogburie, C. P. (2025). The role of cybersecurity in safeguarding finance in a digital era. World Journal of Advanced Research and Reviews, 25(3), 1527–1539.

[6] Bhoomika, S. (2025). An analysis of consumer perspectives on the cybersecurity and data privacy practices in both private and nationalized banks. International Journal of Research Publication and Reviews, 6(8), 1883–1887.

[7] Nair, R. R. (2025). Awareness, threats, and perception of cybersecurity among college students in Thiruvananthapuram District. International Journal of Advanced Research, 13(5), 756–763.

[8] Dwivedi, A., Sharma, P., & Singh, R. (2025). A study of consumer perception towards cybersecurity in online banking. Journal of Emerging Technologies and Innovative Research, 12(5), b155–b174.

[9] Kumbhakar, M. M., & Kumar, N. (2025). Cybersecurity awareness among higher education students in rural India. National Journal of Education, 23(1), 1–10.

[10] Nathe, S. (2025). Investigating the impact of the "Don't Know? Kasih No!" cybersecurity education campaign on digital banking users in Indonesia. International Journal of Security and Safety Engineering, 14(5), 25–40.

[11] Al-Doghan, M. A., & Mirzaliev, S. (2024). Cybersecurity awareness and digital banking adoption: Exploring the moderating impact of digital literacy. International Journal of Economics and Finance Studies, 16(3), 34–58.

[12] Al-Daraba, K., & Sharif, S. M. (2025). Cybersecurity awareness and customer satisfaction in digital banking: A conceptual framework from the Malaysian context. International Journal of Academic Research in Accounting, Finance and Management Sciences, 15(3), 1–18.

[13] Barjaktarovic Rakocevic, S., Rakić, N., & Rakocevic, R. (2025). An interplay between digital banking services, perceived risks, customers' expectations, and customers' satisfaction. Risks, 13(3), 39.

[14] Fatma, D. R., Shukla, K., Bajpai, D. P., & Ahmad, D. S. (2025). Assessing customer's awareness of cybersecurity measures in online banking: A study on digital trust and risk perception. CINEFORUM, 361–386.

[15] Khamis, M. (2025). Examining information security knowledge, attitude, and behaviour among mobile banking users in Zanzibar. East African Journal of Information Technology, 5(1), 1–15.

[16] Bashiru, O. (2023). Exploring mobile banking app security from users' perspectives. International Journal for Information Security Research, 13(1), 1077–1084.

[17] Shah, M., Riasat, I., & Gonul, M. S. (2025). Strengthening cybersecurity resilience: An investigation of customers' adoption of emerging security tools in mobile banking apps. Computers, 14(4), 129.

[18] Paul, O. O., & Ifatimehin, O. O. (2024). Assessing the impact of cybersecurity threats on e-banking adoption in Nigeria. ASRIC Journal of Social Sciences, 5(2), 1–15.

[19] Jisha, T. P., & Sumathy, M. (2024). Exploring the interplay between fintech utilization and cybersecurity awareness. Formosa Journal of Computer and Information Science, 3(1), 41–54.
[20] Sankararaman, G., Suresh, S., Thirumagal, P. G., Priyadharshini, V., & Rengarajan, V. (2024). A study on customer awareness on security issues and threats in digital banking in Chennai. European Economic Letters, 14(4), 559–574.
[21] Krishna, C. P. (2024). A study on cybersecurity threats in digital banking in India. ShodhKosh: Journal of Visual and Performing Arts, 5(1), 2206–2218.
[22] Afzal, M., Ahmad, N., & Ansari, M. S. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India. Journal of Financial Services Marketing, 29(4), 1503–1523.
[23] Renjith, M. J., & Sindoora, S. (2024). Cybersecurity threats in the age of digital banking. Frontiers in Health Informatics, 13(4), 1797–1807.
[24] AlHares, A., Zaerinajad, Z., & Al Bahr, M. (2024). Customer awareness and cybersecurity in OECD countries. Corporate & Business Strategy Review, 5(1), 371–381.
[25] Yuspin, W., Putri, A. O., Fauzie, A., & Pitaksantayothin, J. (2024). Digital banking security: Internet phishing attacks, analysis and prevention of fraudulent activities. International Journal of Safety and Security Engineering, 14(6), 1699–1706.
[26] Almaiah, M. A., Al-Rahmi, W. M., & Al-Rahmi, A. (2023). Investigating the role of perceived risk, perceived security, and perceived trust on smart mobile banking application adoption. Sustainability, 15(13), 9908.
[27] Johri, A., & Kumar, S. (2023). Exploring customer awareness towards cybersecurity in Saudi Arabia. Human Behavior and Emerging Technologies, 5(1), 1–10.
[28] Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The relationship between cybersecurity awareness, knowledge, and behavioral choice protection among mobile banking users in Thailand. International Journal of Computing Sciences Research, 7(1), 1133–1151.
[29] Isa, M. Y. B. M., Ibrahim, W. N. B. W., & Mohamed, Z. (2021). The relationship between financial literacy and public awareness on combating cybercrime in Malaysia. Journal of Industrial Distribution & Business, 12(12), 1–10.
[30] Dam, L. B., & Deshpande, K. (2020). Relationship between demographic variables and awareness on cybersecurity threats. The Orissa Journal of Commerce, 41(2), 112–122.