International Journal of Innovations & Research Analysis (IJIRA)
ISSN :2583-0295, Impact Factor: 6.238, Volume 04, No. 02(II), April- June, 2024, pp 36-42

A STUDY ON CYBER SECURITY AWARENESS IN DIGITAL PAYMENT SYSTEM WITH SPECIAL REFERENCE TO BANASTHALI VIDYAPITH

Mrs. Kavita*
Priyanka Yadav**

ABSTRACT

Overview: *Digital payments are still relatively new in India, and there is always the possibility of a cyber-attack wiping out a person's bank account. Fortunately, the government is hard at work on a highly secure method of making payments using mobile phones and other cashless devices. The Government of India has made digital payment promotion a top priority in order to bring every segment of our country into the formal fold of digital payment services. Technological innovations in the digital payment system are transforming our lives and bringing speed, convenience, choice, and savings to end consumers.*

Purpose: *The Objective of this research is to study and analyse the awareness in public about cyber threats and cybersecurity regarding digital payment and its available solutions and precautionary measures.*

Material and Methods: *Primary data was taken for this study with the help of self structured questionnaire. The authors have used Regression and Correlation to test the hypothesis and SPSS software was used to analyse the responses.*

Result and Findings: *According to the survey, the majority of respondents who use digital payments are educated, and their income status hasn't stopped them from adopting the digital payment system. Respondents have a low level of awareness of cyberattacks. Educated respondents make the best decisions to protect themselves from cyber attacks.*

Conclusion: *According to the study most of the respondents who are using digital payments are educated but they are not completely aware about cyber attacks. Cyber security is still an issue for them that demotivates them to use the Digital financial services. There is a need for enhanced understanding of cybersecurity, cyberattacks, and countermeasures. Educational institutions require cybersecurity since most individuals are unfamiliar with basic cybersecurity concepts or with the best actions to recover their money back.*

Keywords: *Digital Payment, Digital Financial Services, Cyber Security, Cyber Attacks, Cyber Threats.*

Introduction

India's new normal is digitalization. Since demonetization, the government and the Reserve Bank of India have been working hard to build "Digital India". One of Digital India's ostensible functions is "Faceless, Paperless, Cashless." This promotes a cashless economy by allowing people to conduct transactions without using currency. Two things required to foster this cashless economy are smart phones and internet access. Today's world is controlled by smart phones. People use it not just to make calls, but also to buy and sell, make payments transfer money, and so on.

* Research Scholar (Finance), Banasthali Vidyapith, Jaipur, Rajasthan, India.
** Research Scholar, Banasthali Vidyapith, Jaipur, Rajasthan, India.

The Government of India has made digital payment promotion a top priority in order to bring every segment of our country into the formal fold of digital payment services. Technological innovations in the digital payment system are transforming our lives and bringing speed, convenience, choice, and savings to end consumers. During the financial year (FY) 2021-2022, the volume of digital payments in India increased by 33% year on year (YoY). According to the Ministry of Electronics and Information Technology, there were 7,422 crore digital payment transactions in FY 2020-21, up from 5,554 crore in FY 2020-21. As more individuals turn to digital payment it become increasingly vulnerable to dangers and threats (Singh & Rajput, 2018). So, maintaining a careful balance between digital innovation and security is the utmost important. Malware technologies, financial frauds, data breaches, and other dangers are evolving and becoming more complex as sectors become more digital. And, as the digital payments environment has grown in complexity, there has been a growing demand for creative security processes to defend it (Agur et al., 2020). In the sphere of information technology, cyber security is regarded as a critical domain. With all of the threats and vulnerabilities in mind, cyber security emerges as a viable option for mitigating all of these hazards. As cyber-crime has become more prevalent, securing all ends of information has become one of the most pressing concerns (Șcheau et al., 2022). To minimise such crimes to a bare minimum, several strategies and technologies have been developed and used. Despite the various safeguards implemented, many firms are still concerned about cyber security.

In a brief, it is clear that as technology advances, so does the demand for improved cybersecurity for digital payments. Because the advantages of digital payments outweigh the risks, the country must develop a highly secure and convenient digital payments environment. With the government urging residents to switch from cash to digital payments in light of the recent pandemic, fintech companies and the government are expected to work together to improve the sector, making it an essential part of our life (Carley, 2020).

Literature Review

Globalization, aided by information, communication, and technology (ICT), has profoundly altered every aspect of human life in terms of distance and time, presenting governments with both opportunities and challenges. Every country is moving towards the path of digitization in terms of shopping, payment, trading, entertainment, et cetera. Digital technology (big data, wireless technologies, artificial intelligence, virtual and augmented reality technologies) is the foundation of all levels of the digital economy. The formation of an ecosystem has taken place in the electronic payment system. It is technology that enables users with a platform to conduct online payments. The term "digital payment" refers to a system that allows people to conduct financial transactions without the use of cash at any time and from any location. Payment gateways play an important role in the digital payment system. It operates as a mediator, collecting money from users and securely transferring it to the merchant's bank account. A payment gateway is a processor that helps with financial transaction authentication and authorization. To prevent a cyber-attack on the payment system, authentication is essential. A cyber-attack on a financial institution has brought attention to the need to improve cyber-security. Many frauds (like data mining, profiling, exploitation, et cetera.) have been carried out without the consent of users. In the year 2020, Mohammed explained that "Artificial Intelligence" aids in the reduction of cyber security threats. Every year, billions of people throughout the world are impacted by cyber security (*World Bank*, 2020). In this regard, the development of block-chain based identification systems may provide a useful solution to some of the problems that most centralised databases encounter. Furthermore, according to (Tsochev et al., 2020), end users should be given suitable guidelines, such as avoiding clicking on an unfamiliar file or button, and not downloading data from unknown sources. Breaches and fraud can be prevented or minimised by security measures such as firewalls, antivirus software, and employee training, among others. Later in 2021, (Manoj, 2021) has provided some suggestions and recommendations to minimise the cyber risk. The frequency and intensity of cybercrime have been increasing across the globe. It is not only people who are being targeted, but also corporations and governments. To manage the cyber risk, banks and private authorities have been proactively gaining knowledge of the bank’s cyber resilience objective among the customers, vendors, service providers, and other key stakeholders. Banks must take appropriate measures (including developing strong password policies, encrypting sensitive company data, regularly updating the users of the bank, and creating a Safe-Use Flash Drive Policy) to protect the users from cyber-attack.

Research Objectives

- To study demographic characteristics that affect the decision on adoption of a digital payment system.

- To investigate and analyse knowledge of cyber risks and cybersecurity in relation to digital payments.

Target Population

The Study on Cyber Security Awareness in Digital Payment System is done with Special Reference to Banasthali Vidyapith area. The target population is 372 from Banasthali Vidyapith.

Statistical Tools Used for Interpretation and Analysis

The purpose of the study is to study attitudes and behaviour towards digital financial services. A self-structured questionnaire was used to collect the data and there were sub-sections in it. Convenience sampling was used to collect the data from the different sources. The questionnaire was divided into sub-parts.

Part-1 The first part contains the demographic information, including age, gender, income, and employment status.

Part-2 The second part contains the information related to the digital payment system, like which mode you prefer to do digital payment, your most preferred digital payment mode, how frequently you use the digital payment system, etc.

Part-3 The third part contains the information on factors that affect the perception of people using digital payment systems.

Data Collection

For this study, the data is gathered with the help of primary sources.

Primary Source

The primary data were gathered using a self-structured questionnaire, and surveys. The questionnaire was filled through google form and survey method. The questionnaire was distributed offline as well as through google form to the respondents.

Sample Size

The sample size has been calculated with the assistance of Survey System.com.In thecalculator, Iwould betaking confidencelevel 95%, Marginal ofError5%. Thepopulation of Banasthali Vidyapith is 12000.

Coding and Tabulation

After the interview, the information in the questionnaire were edited, and after editing the information each piece of information was assigned a particular number. This is known as Code Manual.

Data Analysis

- The general data of the participants is analysed using descriptive statistics, i.e.frequency distribution and percentage.
- Descriptive statistics, i.e., mean, median and percentage was used to analysis the data.
- Inferential data analysis for hypothesis testing using test statistics: Kruskal-Wallis H test, Spearman's correlation.

Research Results

- Analysis results of demographic characteristics that affects the decision of adoption of digital payment system with special reference to Banasthali Vidyapith.

Based upon the respondents, the majority of the population was female, accounting for 50.2% of the total, and male, 49.8%. 55.6% were 21–30 years of age. Professional is held by 30.8% of the population. 71.3% of respondents were from the category of 250,000-500,000 annual income. 83.2% of people are aware of the availability of digital payment systems. 68.4 % of respondents use their bank's application to use digital financial services. 45.2 % of respondents have been using the digital payment system for more than a year. 44.6 % of respondents are using the UPI to do their transactions. 54.9% of respondents were aware of the phishing cyber-attack. 32% of respondents filled out an online complaint at the relevant bank against a cyber-attack.

H_{01}: There is no significant association of education and the frequently use of digital payment system.

H_{11}: There is a significant association of education and the frequently use of digital payment system.

Table 1 Shows the relationship between the education and frequently use of digital payment system

Education Level * How frequently do you use digital payment? Crosstabulation						
Count						
		How frequently do you use digital payment?				**Total**
		Regulary	**Once a week**	**Once a month**	**Once a year**	
Education Level	Graduation	39	43	18	6	106
	Post- Graduation	65	51	26	1	143
	Research Scholar	77	60	15	6	158
	Professional	85	82	14	0	181
Total		266	236	73	13	588

It was observed that 266 respondents use digital payments use it on a daily basis, 236 respondents use it once a week, 73 respondents use it once a month, 13 respondents use it once a year. This shows that most of the respondents who are using digital payments use it regularly when they need it.

Table 2

Chi-Square Tests			
	Value	**df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	27.198[a]	9	.001
Likelihood Ratio	29.697	9	.000
Linear-by-Linear Association	10.498	1	.001
N of Valid Cases	588		
[a] 4 cells (25.0%) have expected count less than 5. The minimum expected count is 2.34.			

Table 3

Symmetric Measures			
		Value	**Approx. Sig.**
Nominal by Nominal	Phi	.215	.001
	Cramer's V	.124	.001
	Contingency Coefficient	.210	.001
N of Valid Cases		588	
[a] Not assuming the null hypothesis.			
[b] Using the asymptotic standard error assuming the null hypothesis.			

Table 2, 3 reveal that chi-square test of independence showed a significant association education and frequently use of digital payment system with χ^2 (9, 588) = 29.697, p = .000, ϕ = *.215.* The value of phi- coefficient was .215 (<.50) which indicated small effect size. The finding showed that there is a positive effect of education on the frequency usage of digital payment system.

H_{02}: There is no significant relationship between the education and the digital payment mode.

H_{12}: There is significant relationship between the education and the digital payment mode.

Table 4 Shows the relationship between the education and the most preferred digital payment mode

		Which payment mode do you use ?				**Total**
		upi	**E wallets**	**cards**	**E-banking**	
Education Level	Graduation	36	43	18	6	103
	Post- Graduation	65	54	26	1	146
	Research Scholar	77	60	11	6	154
	Professional	85	82	14	5	185
Total		263	239	69	17	588

It was observed that 69 respondents out of 588 are using cards, 239 respondents are using E Wallets, 263 respondents are using UPI Apps, 17 respondents are using E-banking. This shows that very few people are using E-Banking and most of the people are using UPI for digital payments as per the survey.

Table 5

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	26.198[a]	6	.003
Likelihood Ratio	30.697	6	.000
Linear-by-Linear Association	10.498	1	.001
N of Valid Cases	588		

[a] 4 cells (25.0%) have expected count less than 5. The minimum expected count is 2.34.

Table 5 reveal that chi-square test of independence showed significant association education and mode of payment with χ^2 30.697, p = .000, which is less than level of significance 0.05 thefinding showed that there is a positive effect of education on the mode of payment.

H_{03}: There is no significant relationship between the level of income and the desire of taking risk.

H_{13}: There is significant relationship between the level of income and the desire of taking risk.

Table 6 Show the Relationship Between the Level of Income and The Desire Of Taking Risk

			Annual Income in (Rs)	Perceived Risk
Spearman's rho	Annual Income in (Rs)	Correlation Coefficient	1.000	.173**
		Sig. (2-tailed)	.	.000
		N	588	588
	Perceived Risk	Correlation Coefficient	.173**	1.000
		Sig. (2-tailed)	.000	.
		N	588	588

[a] Correlation is significant at the 0.01 level (2-tailed)

Table 6 Spearman's rank order correlation were run to determine the relationship between the annual income and preserved risk There is a positive relationship between the annual income and the desire of taking risk with r = .173, n = 588, p < .000. People having high level of income can take more risk compared to the people having low level of income.

Table 7 Awareness of the Following Cyber Attack

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Phishing	323	54.9	54.9	54.9
	Malware	160	27.2	27.2	82.1
	Ransomware	42	7.1	7.1	89.3
	Social Engineering	63	10.7	10.7	100.0
	Total	588	100.0	100.0	

From table 7 The sample of cyber-attack and digital payments (N = 588), 54.9% of people are aware about the Phishing, 27.2% of people are aware about the Malware, 7.1% of people are aware about the Ransomware, 10.7% of people are aware about the Social Engineering

H_{04}: There is no significant association between the education level and the action taken by users to recover their money back.

H_{14}: There is significant association between the education level and the action taken by users to recover their money back

Table 8 Show the relationship between the education level and the action taken by users to prevent cyber-attack

	Education Level	N	Mean Rank	Median
If you have faced any cyber attack then which kind of action have you taken to recover your money back?	Graduation	106	299.73	3
	Post- Graduation	143	327.38	3
	Research Scholar	158	258.64	2
	Professional	181	296.77	3
	Total	588		3

Table 9

Test Statistics[a,b]	
If you have faced any cyber-attack then which kind of action have you taken to recover your money back?	
Chi-Square	13.652
df	3
Asymp. Sig.	.003
[a] Kruskal Wallis Test	
[b] Grouping Variable: Education Level	

From Table 8,9 To evaluate the difference among the four level of education for behaviour in terms of action against the cyber-attack, Kruskal-Wallis H Test was utilized. The test revealed significant difference in the behaviour among four level of education, *H (3) = 13.652, N = 752 , p = .oo3 , 95% CI.*

Suggestions

- The sample of this study was limited to residents of the Banasthali Vidyapith, but future researchers can collect samples from other institutions to expand the scope of Study and the results should be carefully compared to the data reported in this study
- In the future, the researchers can alter or design a questionnaire that is especially geared to the demands of digital payment and awareness of cyber security.

Conclusion

Educational institutions require cybersecurity since most individuals are unfamiliar with basic cybersecurity concepts or with the best actions to recover their money back. We analysed college students' and staff's cybersecurity awareness at Banasthali Vidyapith, located in Rajasthan via a quantitative research approach. When we analysed the demographic characteristics that affect the decision of adoption of a digital payment system, we found that the majority of participants in the study are educated young people between the age group of 21–30 years who use digital payments, and 83.2% of people are aware of the availability of a digital payment system. Whereas 68.4% of respondents use their bank's application to use digital financial services and 45.2% of respondents have been using the digital payment system for more than a year. Also, it is concluded that there is a significant association between education and the frequent use of digital payment systems, but there is significant association between education and the selection of digital mode. When we looked at risk-taking behavior, we discovered that there is a link between income and the desire to take a risk. It means those who have a high income can easily take the decision to adopt the digital payment system in spite of the risk factor. When it comes to the awareness level of cyber-attacks, people are more aware of phishing attacks than any other type of 54.9%. From the descriptive analysis, 46.1% of people believe that digital payment system should consider the needs and interest of users and provide the products and services they need. It is concluded that there is a significant association between education and action taken by users to recover their money. The level of education plays an important role in cyber security. Those who are educated can easily take action to recover their money. Finally, we concluded that educational institutions should offer security awareness and training workshops on a regular basis to ensure that all users are aware of the most frequent cybersecurity risks and attacks.

References

1. Agur, I., Martinez Peria, S., & Rochon, C. (2020). Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies. *International Monetary Fund*, 1–13.
2. Azhar Mohammed, I. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *International Journal of Innovations in Engineering Research and Technology*, *8*(August), 146598–146612. https://doi.org/10.1109/ACCESS.2020.3013145
3. Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9
4. Digital Financial Service. (2020). In *World Bank* (Issue April).
5. Manoj, K. S. (2021). Cyber Risk in Banking Services: The Extent of Cyber Risks Previsions and Security Measures. *International Journal of Management (IJM)*, *12*(1), 1332–1339. https://doi.org/10.34218/IJM.12.1.2021.117

6. Șcheau, M. C., Rangu, C. M., Popescu, F. V., & Leu, D. M. (2022). Key Pillars for FinTech and Cybersecurity. *Acta Universitatis Danubius*, *18*(1), 194–210.

7. Singh, P., & Rajput, R. S. (2018). Cybersecurity Analysis in the context of Digital Wallets. *International Journal of Advance Studies of Scientific Research*, *4*(3), 522–525. https://ssrn.com/abstract=3355789

8. Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020). Cyber security: Threats and Challenges. *2020 International Conference Automatics and Informatics, ICAI 2020 - Proceedings*. https://doi.org/10.1109/ICAI50593.2020.9311369.

□❍□