Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 2 (2024)

Unveiling the Dark Side of Technology: Understanding the Impact of Cybercrime on the BFSI Sector

Dr. Anita Santosh. Pillai,
Associate Professor, Prin. L.N. Welingkar Institute of Management Development and Research, anita.pillai@welingkar.org

Dr. Hema Doreswamy,
Professor, Prin. L.N. Welingkar Institute of Management Development and Research, hema.doreswamy@welingkar.org

Dr. Jai Raj Nair,
Professor, Prin. L.N. Welingkar Institute of Management Development and Research, jai.nair@welingkar.org

Prof. Roopashree,
Assistant Professor, Vijaya College, roopashreekc6170@gmail.com

Abstract*:*

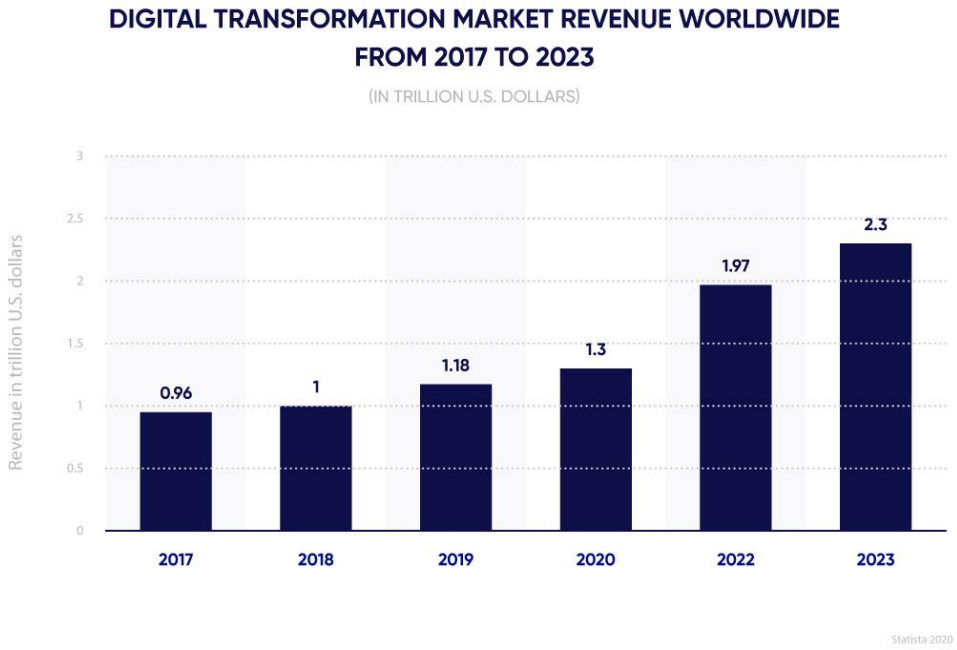
Digital Transformation has brought about unprecedented disruption in the BFSI sector. However, despite the numerous benefits of digitization in banking there are also some inherent challenges. The foremost challenge is the pervasive threat of cyber fraud. Cybercriminals increasingly target banks, individual customers, and financial institutions, resulting in substantial financial losses and posing significant threats to the security and integrity of digital banking systems. To effectively address these threats, it is crucial to understand the various types of cybercrimes. The objective of this study is to examine stakeholders' awareness levels of cybercrimes and preventive measures, assess the cyber security measures adopted by banking institutions, explore users' perceptions of their role in cybersecurity education, and explore the perceptions of the justice system's response to cybercrimes. Statistical analyses, including the Garrett Ranking Conversion Table, T-Test, and ANOVA were conducted to analyze the data. The findings of the study indicate that demographic characteristics significantly influence users' perceptions and response to cybercrimes, highlighting the need for tailored cybersecurity educational campaigns to address diverse needs and awareness levels in a rapidly evolving digital landscape.

Keywords: Cybercrime, Cyber frauds, Banks, Financial Institutions, Cyber security, Online transactions, Preventive measures

Introduction*:*

In recent years, the global BFSI industry has undergone profound digital transformation, revolutionizing how customers interact with the banking services. This evolution has unfolded in different stages – digitization, digitalization and digital transformation. Digitization was the first phase, and it paved the way for conversion of physical customer data into electronic formats. However, this did not enhance the customer experience as transactions still required in-person visits to bank branches. Subsequently digitalization led to utilization of technology to offer enhanced services and new business models. This phase spurred phenomenal growth not only within the banking sector but also across the entire BFSI industry (Banking, Financial Services, and Insurance). Various value-added services offered by the banks changed the customers banking experience totally. With the advent of services like ATMs, customers no longer needed to endure long queues for basic transactions, thereby making banking more convenient and streamlined. Currently we are in the era of digital transformation empowering customers to conduct activities from any part of the world. Internet banking and phone banking have enabled customers to conduct any kind of transaction through their PC or smartphone – be it availing loans, transferring money, investing in capital markets or other investments, buying insurance policies and so on. The Covid-19 pandemic lockdowns accelerated the adoption of these digital services, even among previously hesitant

customers who were reluctant to utilize the value-added services. These customers were either not comfortable with technology, or they had their own fears about adopting these technology-enabled services. The market size of online banking globally stood at $ 11.43 billion in the year 2019 and it is projected to reach $31.81 billion by 2027, with a compound annual growth rate (CAGR) of 13.6%. Digital transformation market revenue worldwide is depicted in the below diagram. It can be observed that the total revenue is increasing rapidly year on year.



(Source: https://light-it.net/blog/digital-transformation-in-banking/)

While the COVID-19 pandemic undoubtedly played a significant role in accelerating the adoption of digital banking platforms, several other factors contributed to this trend. These include widespread smartphone and internet penetration, affordability of internet services, convenience of digital banking transactions, increased returns from online investments, active participation by the corporate sector, and the introduction of innovative services by banks to attract and retain customers.

Key benefits of Digital Transformation of Banking Sector to Stakeholders:

1. Safe and convenient methods available for money transfers
2. Availability of personalized services like financial planning, investments, and tax planning
3. Ease of acquiring and retaining customers through digital marketing.
4. Handling customer grievances in a better manner through customer care centers
5. Faster settlements in investment transactions
6. Automation of routine tasks
7. Banks and financial institutions can gain a lot of insights through data analytics process of transactions which will further help in strategic planning like expansion and new product development.

Though digitization of banking has helped all stakeholders immensely, it has its own limitations. One of the major concerns of digital transformation is cyber frauds. There are many banks, individual customers and other financial institutions who have become targets of cybercrimes and have lost huge amounts of money. Cyber criminals use information and communication technologies with the intention of exploiting personal and financial information of people. Cybercrimes are of different types.

Literature Review:

Businesses face different kinds of risks which can be controllable/internal or uncontrollable/external. Traditionally major business risks were identified as financial risk, interest rate risk, operational risk, default risk, forex risk, and so on. But the entire risk framework has experienced a tectonic shift in the recent past due to huge technological advancements. Now almost all the businesses have exposure to technology. Technology helps businesses in various functions, be it automating the processes, analyzing big data to bring out meaningful solutions, digital marketing, automated payment systems and in many other areas as well. Though these technological interventions largely help businesses, the associated risks are also a reality. Cybercrimes like data theft and financial misappropriations are a cause of major concern. Banks and financial institutions are more vulnerable as perpetrators target these institutions and individuals to gain financially by committing cybercrimes. Rathinaraj, Daniel (2010) et.al confer that though new techniques and compliances are brought into place to combat and eradicate cybercrimes, offenders are coming out with new tools and techniques to commit various cyber offences and cause massive destruction to businesses and loss of wealth to individuals.

BFSI sector has experienced huge transformation in different aspects of operations such as financial products, services, and compliance in the last few decades due to technology adoption. Digitalization has contributed immensely to various stakeholders of BFSI eco-system like customers, bankers, third party operators, regulatory bodies, and government. One of the most important vision and mission of BFSI industry in today's scenario is to come up with innovative solutions to integrate new technology into business operations. "The winners will be the BFSI entities whose leaders are able to align the people and resources to their vision, execute the strategy and implement the ideas faster than others. That means the real challenge involves developing the capability to adopt technology rapidly and responsibly across an organization" (Mark Marone, 2023). There are several notable business transformations as well as social transformations because of successful adoption of technology in BFSI. Technology creates a level playing field as banking services can easily reach the poor and marginalized sections of society. Fintech companies have exhibited the potential of mass reach through digital adoption. Traditional banks and financial institutions are coming up with innovative technology applications to reach out to rural masses. Government, in association, with large technology companies is working towards creating awareness and educating rural population towards financial products and financial services (Kandpal, V., & Mehrotra, R. 2019). Banks are also acting as service aggregators by providing new services to expanding customer base through different electronic delivery channels. Financial inclusion is a major agenda of every government, especially in emerging economies. This has opened new horizons for banks and financial institutions to expand their business operations by creating innovative products and services. Technology plays a pivotal role in creating competitive edge for these banks and financial institutions (Sriya P, 2014). A robust financial system and well-equipped banking institutions are the hallmark of a growing economy. Effective mobilization of deposits and smooth flow of credit to the needy, be it industry or individuals has become a reality due to effective adoption of technology by BFSI sector (Shetty, Megha & K., Nikhitha, 2022). It is an obvious fact that adoption of technology in BFSI has brought in a tectonic shift in the banking business and has created complete transformation in the BFSI operations for all stakeholders – banks, customers, investors, employees and so on. Though technology in BFSI has impacted the entire industry positively and has changed the landscape of the banking industry by leaps and bounds, this is not devoid of demerits and risks. As BFSI is becoming more and more technology driven, the sector is vulnerable towards sophisticated cybercrimes. The landscape of cybercrimes includes data breaches, malware attacks, ransom attacks, conning customers and siphoning their money, and so on. In the current scenario, cybersecurity is the topmost concern for the industry. (Kohli, Karmendra 2023). Cybercrimes are also evolving in tandem with technology advancement in BFSI. The attackers keep researching and studying the existing technology application in banking sector and ultimately find some loopholes which they will exploit (Batra, Narendra Kumar Parul, Gulati 2022). An exclusive report by SaaS security firm Indusface shows that Indian BFSI sector was hit with over 140 million cyber-attacks in the month of February 2023 alone. The report also highlights that the insurance sector is more vulnerable than the banking industry and attracts more cyber-attacks. Increased cyber-attacks on banks and financial institutions have caused loss of goodwill and have impacted the economy negatively. The solution to this problem is two-fold. The first is coming up with technical products/warning systems which can minimize these attacks and second is to create awareness among users of financial products and services. The massive losses arising due to cybercrimes need to be

countered and prevented (Akinbowale et al., 2020). One major factor for such frequent cyber-attacks is lack of awareness among customers in keeping their bank accounts secured and revealing key information when fraudsters trick them by luring them to share their passwords and other sensitive details. There is an urgent need to educate BFSI customers on various types of financial frauds/cyber-attacks and how to handle confidential financial data in the present online banking system. They should be trained in defending themselves against online financial frauds and cyber-attacks. (Manivannan, et al., 2020). Criminal activities related to the internet are termed cybercrimes. With the increased popularity of online business and online banking transactions, it is important to provide legal cover to the victims and punish the perpetrators. The branch of law which deals with cybercrimes is what is referred to as cyber law. Though it is impossible to avoid cybercrimes totally, there exists a rule of law which can be used to punish the fraudsters (Kapila, Pallavi 2020). Analysis of cyber violations during Covid-19 period shows a staggering increase in the number of attacks. Women are the major target of such cyber-attacks. Due to Covid-19, there was an increased participation of citizens in the online space, in general, and online banking transactions in particular. This could also be a reason for the increase in cybercrimes during Covid-19. (Kumar Sanjeev, Manhas Anupam, 2021).

Research Objectives:
After a detailed and through review of existing literature, the objectives of the study were finalized as follows:

- To examine the awareness levels among stakeholders regarding various types of cybercrimes and the efficacy of preventive measures.
- To explore the perception of users towards their responsibility in educating themselves about cybersecurity measures and practices.
- To study the perception of users regarding the legal system against cybercrimes

Research Methodology:

The study was conducted in Bengaluru, India to examine the impact of cybercrimes on BFSI sector. The study is based on primary data. A structured questionnaire was administered to collect the data. 130 questionnaires out of the total responses received were considered for analysis. The questionnaire focused on the following components: demographic details, awareness about types of cybercrimes, whether a victim of cybercrime and if yes, what type of cybercrime, knowledge of preventive measures, and perception on the awareness campaigns on cybercrimes by the government, banks and financial institutions or any other member of the ecosystem.
To check the internal consistency and reliability of the questionnaire, Cronbach's Alpha test was conducted, and the value was greater than 0.70 which is acceptable to carryout the study further.
The collected data was analyzed using statistical tools like percentage analysis, descriptive statistics, chi-square test, t-test, and word cloud to bring out meaningful insights.

Hypotheses:
The following are the main hypotheses tested in this study.

1. H_0: There is no significant association between demographic factors and the perception of internet users against cybercrimes.
2. H_0: There is no significant difference between the level of awareness regarding types of cybercrimes and preventive measures.
3. H_0: There is no significant difference between the perceptions of internet users on responsibility to educate themselves about cyber security, justice against cybercrimes.

Data Analysis and Interpretation:
This section covers analysis conducted by using appropriate statistical tools. The data is also represented in charts and graphs. Based on the analysis, hypotheses testing, findings and inferences are listed.

Table 1: Percentage Analysis of the Socio-demographic factors

		Gender	Occupation	Qualification	Annual Income
	Valid	130	130	130	130
N	Missing	0	0	0	0

Source: Compiled from Primary data

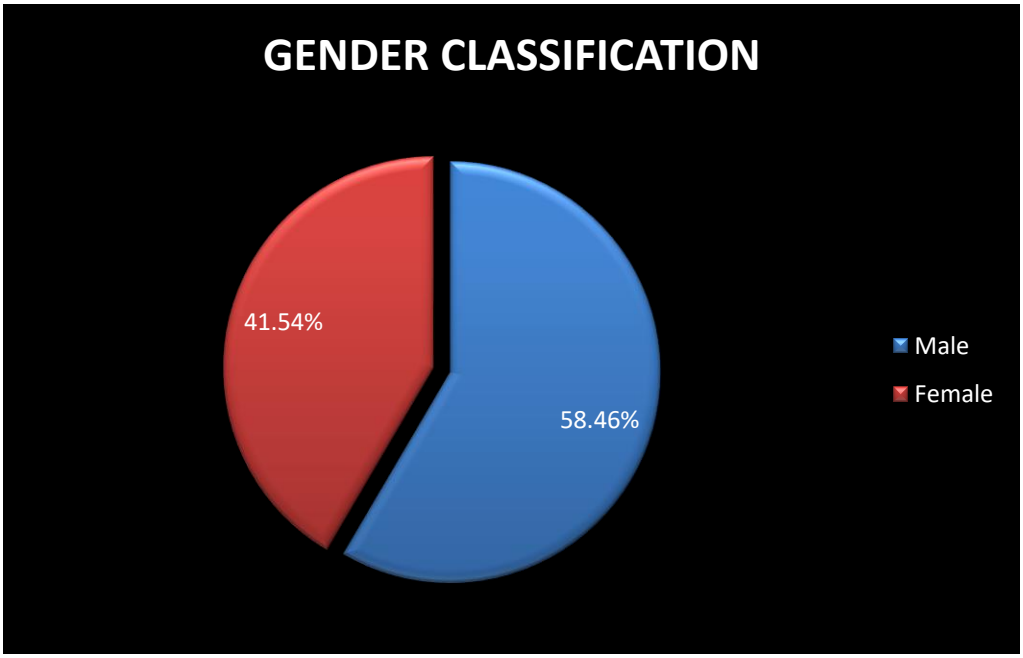
Table 2: Percentage Analysis of the Socio-Demographic Statistics – Gender Classification

	Gender	Frequency	Percentage	Cumulative Frequency
Valid	Male	76	58.46	58.46
	Female	54	41.54	100.00
	Total	130	100.00	

(Source: Compiled from Primary data)

Table 2 exhibits the demographic factors of gender classification shows that 58.46% of the respondents are males and 41.54% are female respondents.

Chart 1: Gender Classification



Source: Compiled from primary data

Table 3: Percentage Analysis of the Socio-Demographic Statistics – Occupation

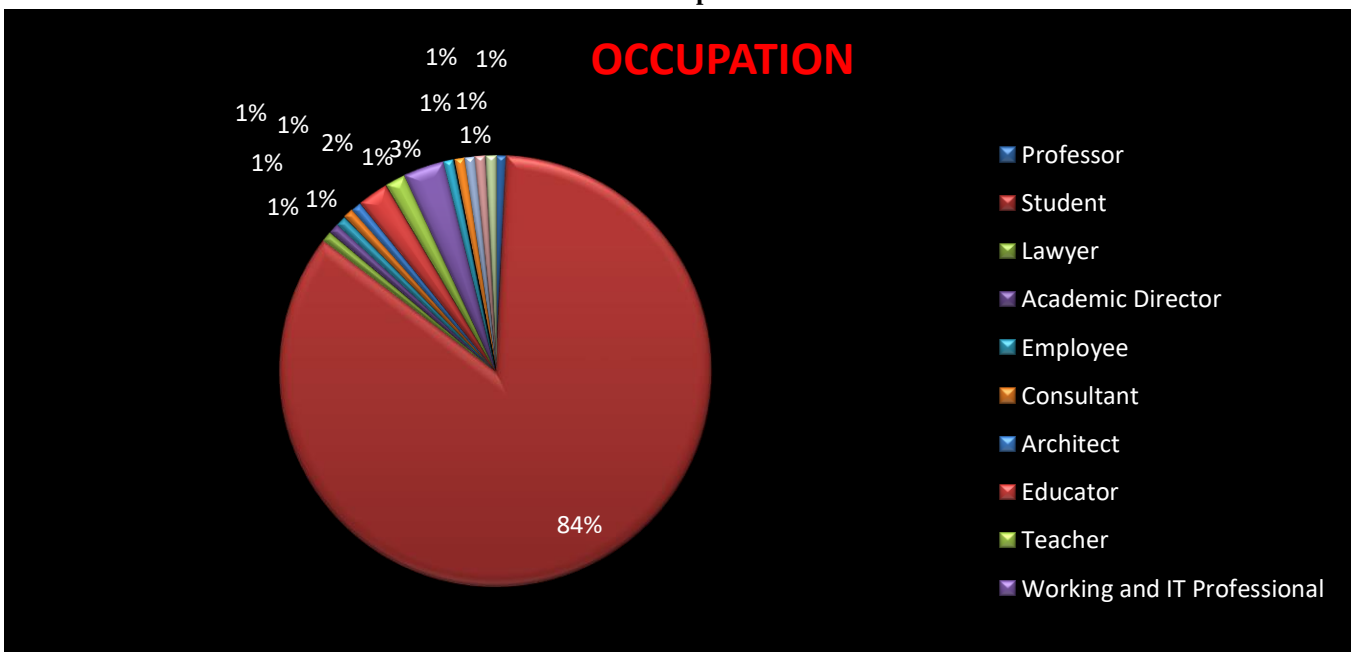
	Occupation	Frequency	Percentage	Cumulative Frequency
Valid	Professor	1	0.769	0.769
	Student	110	84.614	85.383
	Lawyer	1	0.769	86.152
	Academic Director	1	0.769	86.921
	Employee	1	0.769	87.690
	Consultant	1	0.769	88.459
	Architect	1	0.769	89.228

	Educator	3	2.307	91.535
	Teacher	2	1.538	93.073
	Working and IT Professional	4	3.082	96.155
	Entrepreneur	1	0.769	96.924
	Academician	1	0.769	97.693
	Research associate	1	0.769	98.462
	Writer	1	0.769	99.231
	Engineer	1	0.769	100.00
	Total	130	100.00	

Source: Compiled from Primary data

Table 3 enumerates the results of occupation. Where the maximum numbers of respondents are students whose percentage is 84.614% followed by working and IT professional as 3.082% and Educator as 2.307% respectively.

Chart 2 Occupation



Source: Compiled from Primary data

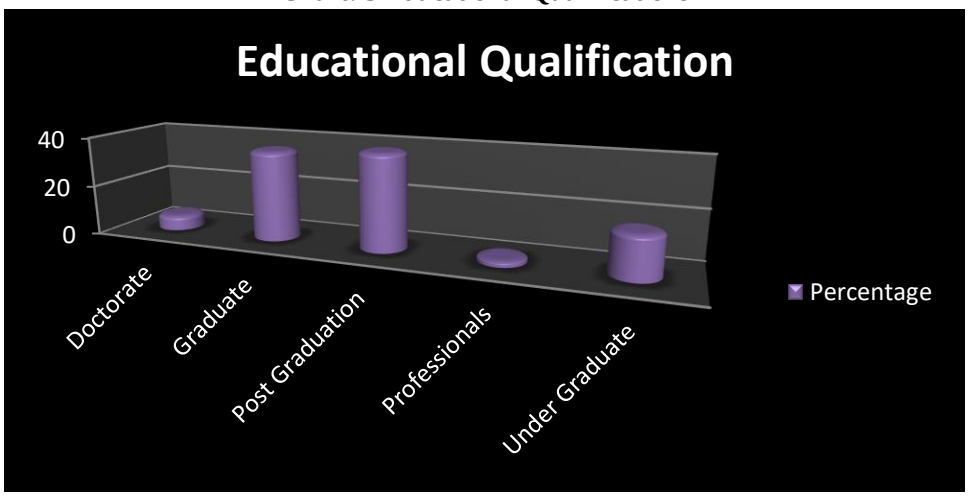
Table 4: Percentage Analysis of the Socio-Demographic Statistics – Educational Qualification

	Occupation	Frequency	Percentage	Cumulative Frequency
Valid	Doctorate	8	6.153	6.153
	Graduate	47	36.153	42.306
	Post Graduation	50	38.464	80.77
	Professionals	3	2.307	83.077
	Under Graduate	22	16.923	100.00
	Total	**130**	**100.00**	

Source: Compiled from Primary data

Table 4 describes the different Educational Qualification; where the maximum number of 38.46% of respondents is from PG followed by Graduate as 36.153% and the minimum number of respondent's lies with professionals as 2.307% respectively.

Chart: 3 Educational Qualifications



Source: Compiled form Primary data

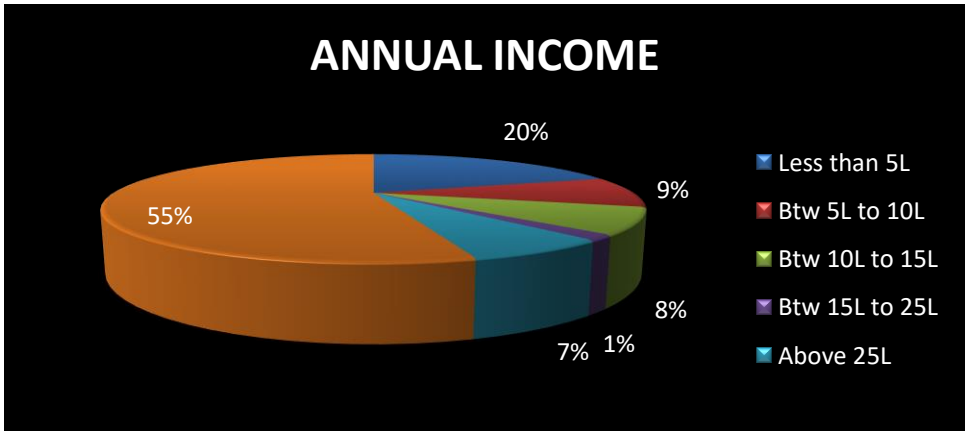
Table 5: Percentage Analysis of the Socio-Demographic Statistics – Annual Income

	Annual Income	**Frequency**	**Percentage**	**Cumulative Frequency**
Valid	Less than 5L	26	20.00	20.00
	Btw 5L to 10L	12	9.230	29.23
	Btw 10L to 15L	10	7.694	36.924
	Btw 15L to 25L	2	1.538	38.462
	Above 25L	9	6.923	45.385
	Not applicable	71	54.615	100.00
	Total	**130**	**100.00**	

Source: Compiled from Primary data

Table 5 considering the different Annual Income, where many of the respondents with 20% lies with less than 5 Lakhs followed by between 10Lakhs to 15Lakhs with 7.694%. But many of them are in the range of Not applicable with 54.61% respectively.

Chart: 4 Annual Incomes



Source: Compiled from Primary data

H_0: There is no significant association between Demographic Factors and the Perception of Internet Users against Cybercrimes

Table 6: Association between Demographic Factors and the Perception of Internet Users against Cybercrimes

Demographic Factors	Chi-Square test		Strength of Association		
	Pearson Chi-Square	Asymp.Sig	Phi	Cramer's	Sig.
Gender	3.815	**0.000****	0.128	0.288	**0.000****
Educational Qualification	22.61	**0.000****	0.948	0.948	**0.000****
Occupation	18.69	**0.000****	0.083	0.061	**0.000****
Annual Income	71.92	**0.000****	0.193	0.492	**0.000****

Source: Compiled from Primary Data of 130 respondents
****Phi and Crammers lie between 0 to 1 are a closer association**

Table 6 denotes the results of association between factors and the perception of internet users against cybercrimes. It is interpreted that all the selected demographic factors are less than the significant value 0.05 with Chi.Square value of 3.815, 22.61, 18.69, 71.92 respectively. Hence, the null hypothesis is rejected, and it is concluded that there is significant association between the Demographic factors and Perception of Internet users against cybercrimes. Phi and Crammers V indicate the strength of the relationship between the variables. A significant Phi and Crammers V is higher than 0.25 indicate the strong relationship with Gender, Qualification, and Annual Income. According to this result educational Qualification has a strongest association with the perception of Internet users against cybercrimes.

Objective 1: To examine the level of awareness with regards to types of cybercrimes and preventive measures
H_0: There is no significant difference between the level of awareness with regard to types of cybercrimes and preventive measures

Table 7: independent sample t-test for the level of awareness concerning cybercrimes

Awareness concerning about cybercrimes	Levene's Test for Equality of Variances			t-test for equity of means				
	f	R^2	Sig	t	df	Sig (2 tailed)	Mean difference	Std.Error
Equal Variance Assumed	0.282	0.592	0.014	3.979	129	**0.000****	46.716	11.839
Equal Variance are not Assumed				4.028	94.141	**0.000****	45.940	10.127

Level of significance of 0.05**
Source: Compiled from Primary Data of 130 respondents

Table 7 reveals the results of independent t sample for the level of awareness concerning cybercrimes. Based on the results, it is demonstrated that the R square value is 0.592 and it has 59.2 percent of variance and has a remarkable effect with level of awareness regarding cybercrimes. Where, the t value of significant variance is less than 0.05 and is concluded that there is a significant difference between the level of awareness with cybercrimes and preventive measures.

Table 8 Results of ANOVA for the level of awareness concerning cybercrimes

Variables	Labels	SS	MS	F	Sig.
aware of anyone	Between Groups	11.838	3.391	2.111	**0.004****

in your circle who has been a victim of cybercrime	Within Groups	87.041	2.157		
	Total	**98.879**			

Level of Significance of 0.005**
Source: Compiled from Primary Data of 130 respondents

Table 8 shows the results of ANOVA for the level of awareness concerning cybercrimes. Since the p value is lesser than the significant value of 0.05, there is a significant difference with the awareness as to who has been a victim of cybercrime.

(i) Word Cloud for the level of awareness about types of cybercrimes and preventive measures

Source: Compiled from Primary data

Factors extracted from Word Cloud

S.no	List of words Extracted
1.	Phishing
2.	Malware
3.	Hacking
4.	Theft
5.	Ransomeware
6.	Social Engineering
7.	DOS Attacks
8.	Financial Frauds
9.	Shared OTP
10.	Credit Card Frauds
11.	Fraudulent Business Practices
12.	Threat Calls
13.	False Pretense
14.	Cyber Hacking
15.	Debit Card Fraud

Objective 2: To determine cyber security preventive measures adopted

Table 9: Garret Ranking Conversion Table for active implementation of Preventive measures

Variables	Percentage	Score
Using strong passwords	**99.03**	**2**
Using unique passwords for different online uses	96.99	4
Enabling two-factor authentication	92.45	6
Keeping software and operating system up-to-date	94.42	5
Taking regular backup of data	81.99	9
Ignoring suspicious emails and links	**97.72**	**3**
Using anti-virus	83.31	8
Encrypting sensitive data	86.69	7
All the Above	**99.62**	**1**

Source: Compiled from Primary Data of 130 respondents

Based on the Garret Ranking results enumerated from the table 9, it is interpreted that variables include all the above are ranked 1st with 99.62 percentage, using strong passwords were ranked as 2nd with 99.03 percent and ignoring suspicious emails and links has ranked 3rd with 97.72 percent and the least ranking shows in using anti-virus with 83.31 percentage by 8th rank respectively.

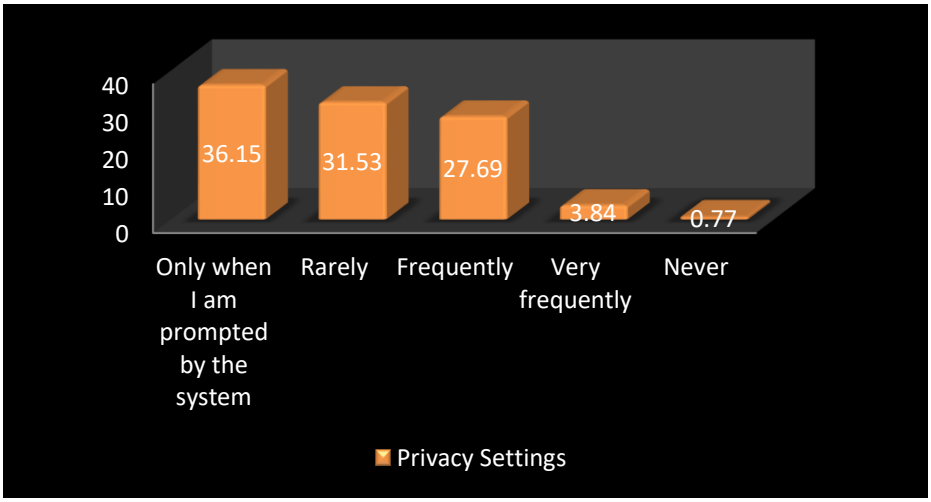
Objective 3: To study the perception of internet users on responsibility to educate themselves about cyber security and preventive measures.

Table 10 Descriptive statistics for Privacy Settings on Social Media Platform

	Privacy Settings	Frequency	Percentage	Cumulative Frequency
Valid	Only when I am prompted by the system	47	36.15	36.15
	Rarely	41	31.53	67.68
	Frequently	36	27.69	95.37
	Very frequently	5	3.84	99.23
	Never	1	0.770	100.00
	Total	**130**	**100.00**	

Table 10 describes the descriptive statistics for privacy setting on social media platforms. The results enumerate that many of the respondents i.e. 36.15 percent change their privacy setting only when they are prompted by the system while 31.53 percent rarely update their privacy settings. However, 27.69 percent users frequently change the privacy setting on social media and miniscule users (3.84%) change their privacy settings very frequently.

Chart: 5 Privacy Settings on Social Media Platform



Source: Compiled form Primary data

Table 11: Word Cloud regarding information about latest cyber threats and preventive measures

S.no	List of words Extracted
1.	Newspaper
2.	Cyber scams
3.	Social media
4.	Friends and family
5.	Technological advancements
6.	Updating software
7.	Blogs and YouTube
8.	Tracking
9.	Cyber security laws
10.	Cyber Awareness
11.	Punishable justice
12.	Cybercrime footprints

Source: Compiled from Primary data

H0: There is no significant difference between the perceptions of internet users on responsibility to educate themselves about cyber security, justice against cybercrimes

Table 12: Results of the Difference between the perceptions of internet users on responsibility to educate themselves about cyber security, justice against cybercrimes

Variables	Labels	N	Mean	t-stat	Sig.
responsibility to educate themselves about online security and preventive measure	Yes	127	2.071	0.309	**0.041****
	No	3	0.112		
Cybercrime be brought to justice	Yes	105	1.849	1.113	**0.000****
	No	25	0.524		
interested in attending workshops and/or seminars on cyber security and online safety	Yes	69	1.251	1.464	**0.000****
	No	6	0.053		
	May be	55	1.759		
Participated in any cybercrime awareness programs or initiatives in the past one year?	Yes	21	0.623	2.990	**0.000****
	No	109	1.709		

Source: Compiled from primary data of 130 respondents, **0.05 level of significance

Table 12 shows the results of the Difference between the perceptions of internet users on responsibility to educate themselves about cyber security, justice against cybercrimes. It is observed that all the select variables have a significant association with 'educate themselves about cyber security' and 'justice against cybercrimes and the values are less than the significant p value of 0.05.

Conclusion:

Digital wallets and online payment methods have significantly contributed to the evolution of a less-cash society. However, the proliferation of real-time online transactions and the digital payment ecosystem has correspondingly spurred a global increase in cybercrimes. Fraudsters are constantly devising innovative methods to hack and execute cybercrimes. This study reveals that demographic characteristics significantly influence how internet users perceive and respond to cybercrimes. There is a notable correlation between an individual's level of education and their perception of cybercrimes. Furthermore, awareness and knowledge about cybercrimes vary considerably depending on the specific type of cybercrime. The understanding and implementation of preventive measures also differ among individuals, with some preventive measures being more widely known and commonly practiced than others.

Additionally, users have diverse opinions regarding the adequacy of current laws and regulations in addressing and preventing cybercrimes.

The research findings underscore the necessity of considering demographic diversity when designing and implementing cybersecurity policies, educational campaigns, and protection strategies. It is crucial to develop targeted educational campaigns and training programs that address specific types of cybercrimes and their respective preventive measures. A one-size-fits-all approach to cybersecurity awareness is unlikely to be effective, as different types of cybercrimes and preventive actions require varying levels of emphasis and education. Therefore, a more tailored approach that is sensitive to the diverse demographic factors, is essential for enhancing cybersecurity awareness and protection.

References:

1. Rathinaraj, D., & Chendroyaperumal, C. (2010). Financial fraud, cyber scams and India–A small survey of popular recent cases. *Cyber Scams and India–A Small Survey of Popular Recent Cases (May 12, 2010)*, SSRN Electronic Journal, May 2010DOI:10.2139/ssrn.1605165
2. Kandpal, V., & Mehrotra, R. (2019). Financial inclusion: The role of fintech and digital financial services in India. *Indian Journal of Economics & Business*, *19*(1), 85-93.
3. Siriya, P. (2024), Technology an Important Driver in BFSI Sector, Abhinav International Monthly Refereed Journal of Research in Management & Technology, Volume 3, Issue 4, 46-55
4. Shetty, Megha & K., Nikhitha. (2022). Impact of Information Technology on the Banking Sector. International Journal of Management, Technology, and Social Sciences. 634-646. 10.47992/IJMTS.2581.6012.0241.
5. Kumar Narendra, Gulati Parul (2022) Cyber Attacks on Banking Institutions in India: Safety and preventive measures, International Journal of Innovations & Research Analysis (IJIRA) 19 ISSN: 2583-0295, Impact Factor: 5.449, Volume 02, No. 02, April - June, 2022, pp 19-23
6. Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020), "Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature", *Journal of Financial Crime*, Vol. 27 No. 3, pp. 945-958.
7. Manivannan, Adharsh & Moorthy, Dhatchina. (2020). Cyber Attacks in the Banking Industry, December 2020, Conference: Cyber-attacks in banks at Bournemouth, England
8. Kapila, Pallavi (2020) Cyber Crimes and Cyber Laws in India: An Overview, In book: Contemporary Issues and Challenges in the Society (pp.36-48), Edition: 2020, Publisher: New Era International Imprint
9. Sanjeev Kumar, & Dr Anupam Manhas. (2021). CYBER CRIMES IN INDIA: TRENDS AND PREVENTION. *Galaxy International Interdisciplinary Research Journal*, *9*(05), 363–370. https://doi.org/10.17605/OSF.IO/HC4RZ
10. BFSI's Digital Transformation Is Not All About Technology - Harvard (harvardbusiness.org)
11. Navigating the Shifting Landscape: BFSI Sector Leaders' Key Concerns and Challenges (cxotoday.com)
12. Exclusive: Indian BFSI sector faced over 140M cyberattacks in 1 month, ET CISO (indiatimes.com)
13. Digital Transformation in BFSI Future & Trends, Benefits (motivitylabs.com)
14. https://www.alliedmarketresearch.com/online-banking-market