

An Empirical Study On Awareness Of Cyber Security In Digital Banking Among College Going Students (With Special Reference To Korba District Of Chhattisgarh)

OPEN ACCESS

Volume: 3

Issue: Special

Month: May

Year: 2024

ISSN: 2583-7117

Published: 07.05.2024

Citation:

Manharan Anant¹, Kalpana Kanwar², Dr. Sushil Kumar Indulkar³. "An Empirical Study On Awareness Of Cyber Security In Digital Banking Among College Going Students (With Special Reference To Korba District Of Chhattisgarh)." International Journal of Innovations In Science Engineering And Management, vol. 3, Issue: Special, 2024, pp. 45–49.



This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Manharan Anant¹, Kalpana Kanwar², Dr. Sushil Kumar Indulkar³

¹Assistant Professor, Department of Commerce, Govt Naveen College, Jatga, Dist. - Korba, C.G.

²Assistant Professor, Department of Commerce, Govt. E.V.P.G College Korba, Distt. Korba, C.G.

³Assistant Professor, Department of Management, Pt. Ravishankar Shukla University Raipur, Distt. Raipur, C.G.

Abstract

Now a day it become a common practice of many people to use the internet through computer or mobile for any banking activities because we all are living in the age of information and communication technology era. For digital banking, many apps were used such as Google Pay, PhonePe, Paytm, BHIM, NEFT, UPI etc. The number of online-banking users are rising rapidly, everyone is very much dependent upon the cyber world which also increases the chance of cybercrime. The term cybercrime means when a person using internet to access information of others without his permission with an intention to harm him or her. Cybercrime is related to ATM, DEBIT card and net banking. As compared to other sector, banking sector is more facing problem relating to cyberattacks. Due to such an individual and organization, both should take all precautions to minimize cyberattacks. This paper aims to raise awareness about cybercrime and cybersecurity. It endeavors to assess the awareness of college students in Korba district, Chhattisgarh, regarding cybersecurity in the banking sector.

Keyword: Cyber Crime, Cyber Attacks, Digital banking.

1. INTRODUCTION

Cybersecurity holds immense significance within the realm of Information Technology, with businesses and financial institutions alike prioritizing safeguarding their digital assets. In the contemporary landscape, where over 60% of commercial transactions in India occur online, the risk of cybercrime looms large. Recognizing this threat, governments worldwide have enacted stringent laws to combat fraudulent activities and protect sensitive information. In the sphere of banking and financial transactions, technological advancements and robust infrastructure are pivotal for national development, especially among emerging economies. The internet has emerged as a symbol of progress, revolutionizing traditional banking with its user-friendly interfaces and enhanced flexibility in payments and transactions. Through online and core banking systems, customers now enjoy unparalleled convenience, accessing information and making financial decisions with a mere click, eliminating the need for physical mobility.

However, this digital convenience also exposes users to potential cyber threats if they remain unaware of security protocols and legal protections offered by financial institutions. Recognizing this vulnerability, banks and financial service providers have fortified their defenses with multi-layered security measures, aiming to shield customers from cyber-attacks. Moreover, extensive awareness programs on cybersecurity and cybercrimes have been initiated to empower users with the knowledge necessary to navigate the digital landscape safely. In essence, the evolution of Information Technology has brought unprecedented convenience and accessibility to financial services, yet it has also necessitated a heightened focus on cybersecurity to mitigate risks and ensure the integrity of digital transactions.

The Reserve Bank of India (RBI) has issued instructions to banks to enhance security measures at their branches and ATMs to mitigate cybercrime risks. Despite customers displaying relatively fewer challenges in terms of Information Technology proficiency, the task of regular checks and monitoring has become increasingly intricate due to the surge in online transactions. In today's technologically advanced world, the evolution of technology has not only transformed business operations but has also significantly impacted the Indian financial sector, particularly banking operations. This technological advancement has contributed qualitatively and quantitatively to the country's development, notably through the rapid expansion of data operations and sciences, thus enhancing the standard of living.

Given that the banking industry serves as the cornerstone of the Indian financial system, it has played a pivotal role in fostering economic growth and development. The integration and utilization of technology in banking operations, such as automated core banking and cloud banking services, have propelled the adoption of online banking by customers.

However, alongside technological progress, there has been a concurrent rise in cybercrimes and digital frauds, where unsuspecting customers are deceived. Thus, there is a pressing need to prioritize protection, prevention, and awareness against these cybercrimes and digital payment frauds, particularly focusing on shielding customers from counterfeit online banking systems. This study is grounded in the Indian context, emphasizing the dynamic relationship between bankers and customers in online banking services and underscores the importance of security measures in thwarting online financial crimes. The research highlights ample scope for examining and evaluating bank customer awareness concerning cybersecurity and digital payment fraud prevention, especially within nationalized banks.

II. LITERATURE REVIEW

Urna Butchi Babu (2018) The government's support following the demonetization in November 2016 has resulted in a remarkable increase in new digital banking customers, and digital payments have experienced unprecedented growth, setting record levels. May mobile applications were developed by bank for bill payments, 24x7 money transfer facility etc.

Mirdul Sharma and Satvinder Kaur (2019) state that Cybercrime has emerged as a serious threat to society, with a significant number of individuals falling victim to hackers

who exploit vulnerabilities to gain unauthorized access and steal both data and money. These cybercriminals capitalize on the advancements in technology to profit from illicit activities.

According to Subodh Kesharwani (2019), the current landscape witnesses a rise in cyber security concerns, leading to an escalation in issues surrounding digital privacy. As cyber-attacks emerge as a global menace, organizations are compelled to devise innovative strategies within the digital realm to combat such threats, with particular emphasis on the banking sector.

In their 2020 study, Gupta Nakul and Jhamb Dharmender offer valuable insights into fraud mechanisms. By identifying loopholes and proposing relevant policy interventions, the paper traces the evolutionary history of fraud and presents preventive tools to curb its diverse manifestations. The authors emphasize the importance of prioritizing interventions, delineating them clearly, and assessing their effectiveness and potential for inducing change.

III. OBJECTIVE OF THE STUDY

The following are the objective of research:

- To study the level of cyber security awareness in banking sector among college going student of Korba district of Chhattisgarh.
- To find out how demographic and socio – economic factors affect the level of awareness of cybersecurity in banking sector among students of Korba district.

IV. HYPOTHESIS

To facilitate research, the following hypotheses have been formulated:

Hypothesis 1

H0: There is no significant impact of gender on the level of cybersecurity awareness in the banking sector.

Hypothesis 2

H0: There is no significant impact of location on the degree of cybersecurity awareness within the banking sector.

V. METHODOLOGY

For the purposes of the studies, a questionnaire-based survey was conducted amongst college going students of Korba district. The questions were constructed to conclude

the participant's familiarity with cyber security issues. Students of different college were invited to participate in the study. The link of questionnaires was sent through WhatsApp and other social media platforms to the student registered under any college of Korba. Participants were encouraged to share this link with as many people as possible. Participants were automatically led to details about the study and informed consent after obtaining and clicking the connection.

The major objectives of the study is to discover the association between socio- economic factors and awareness level of cyber security among the college going of Korba. The hypothesis of this paper was tested with the help of Mean, Standard Deviation, and ANOVA.

VI. DATA ANALYSIS & INTERPRETATION

Gender	N	Mean	SD	P -value	Significant value
Male	298	88.1	11.4	0.55	0.001
female	252	88.7	10.3		

Table: 1 cybersecurity awareness in the banking sector as per Gender

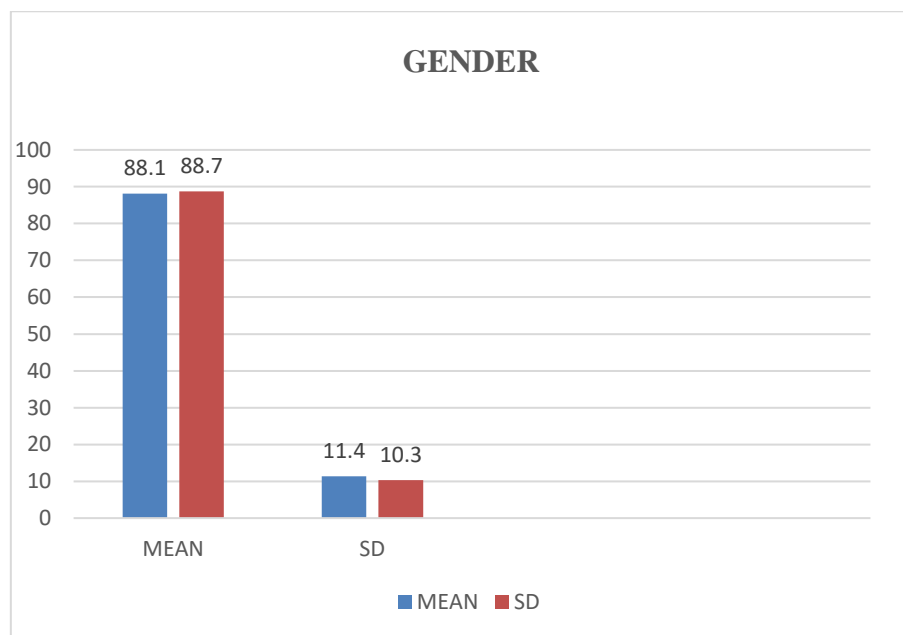


Table: 1 Indicates that the mean scores of male for awareness for cybersecurity is 88.1 and the mean scores of female for cybersecurity is 88.7 and their SD values are 11.4 and 10.3 respectively. The p-value exceeding the

predetermined significance level leads to the acceptance of the null hypothesis. Thus, it is inferred that there exists no notable difference in the level of awareness among students regarding online banking.

RESIDENCE	N	MEAN	SD	P value	Significant level
URBAN	234	90.7	10.17	0.0002	0.01
RURAL	316	86.0	11.7		

Table: 2 cybersecurity in the banking sector in Urban and Rural areas

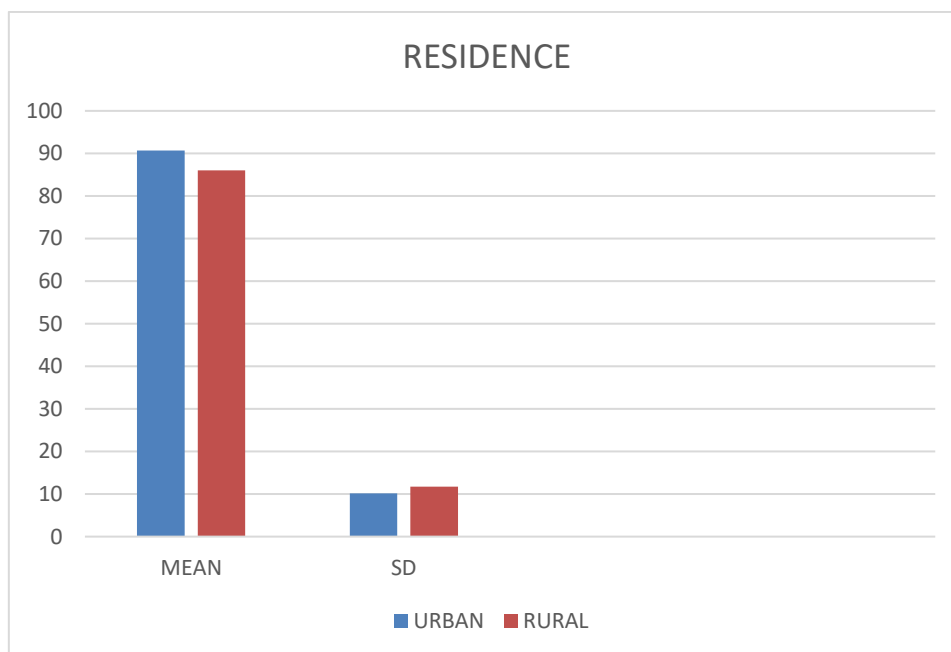


Table: 2 Indicates that the mean score of student belong to urban area is 90.7 and the mean score of students belong to rural area is 86.0 for awareness of cyber security in banking sector and their SD is 10.17 and 11.7, the value of p is less than the significant level .hence null hypothesis is rejected . Which mean location affect the level of awareness.

VII. FINDINGS OF THE RESEARCH

The primary conclusions of the study stem from an examination conducted on the data obtained from respondents through a research survey regarding customer awareness of safety, security, and cybercrimes and frauds in online banking, specifically within Nationalized Banks in Korba city. These findings are organized according to demographic profiles and study variables analyzed within the research. Below are the main findings:

- A survey reveals that 40.1% of the respondents are currently utilizing e-banking services and are well-versed with its functionalities. Additionally, 28.3% of participants have adopted online banking based on recommendations from their family and friends, while 21.8% have been influenced by advice and endorsements from bank officials.
- Regarding the purpose of online banking usage, 31.4% of respondents utilize it for personal transactions, 25% for online money transfers (NEFT/RTGS), 20% for bill payments, 13% for regular banking transactions, and 11% for online shopping.

- Furthermore, the study indicates that 35.3% of respondents consistently use online banking for all their transactions, 29% use it occasionally, 16.7% rely on it for every transaction, and the remaining 18.7% either use it sporadically or not at all.

VIII. CONCLUSION

Over the past two decades, there has been remarkable growth in information and technology, fostering innovation across all business sectors. This transformation has significantly impacted the financial sector, which serves as the foundation for all business operations. Within the banking industry, these advancements in technology and financial innovations have simplified transactions for customers, catering to their diverse financial and retail needs. Consequently, technological progress has led to advancements in banking operations.

Despite the array of electronic banking services offered to end-users, there are notable drawbacks concerning the complete security and privacy of online banking. While these services aim to enhance convenience and accessibility for customers, they also introduce vulnerabilities that jeopardize the security and confidentiality of online transactions.

According to the result analysis, it was identified that students of rural areas need more attention toward banking technology.

References

- Chakraborty, S. (2019). Malware attack and malware analysis: A research. *International Journal of Scientific Research in Computer Science*, 5(3), 268-272.
doi:10.32628/CSEIT195379
- Choucrist, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, 20(2), 96-121. DOI:10.1080/02681102.2013.836699
- CNSS. (2010). National Information Assurance (IA) Glossary CNSS Instruction No. 4009. Washington DC: Committee on National Security Systems (CNSS) Glossary Working Group. <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>
- Dunkels, E. (2008). 'Children's Strategies on the Internet.' *Critical Studies in Education*; 49(2), 171-184. <https://doi.org/10.1080/17508480802123914>
- Educause. (2015). Top 5 strategic information security issues for 2015. Louisville: Educause. <https://er.educause.edu/articles/2015/1/top-10-it-issues-2015-inflection-point>
- Erbschloe, M. (2019). Social engineering: Hacking systems, nations, and societies. Boca Raton: CRC Press <https://doi.org/10.1201/9780429322143>
- F. Alotaibi, S. Furnell, I. Stengel and M. Papadaki, (2016) "A survey of cyber-security awareness in Saudi Arabia," 11th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 154-158, doi: 10.1109/ICITST.2016.7856687.
- Furnell, S., & Vasileiou, I. (2017). Security education and awareness: Just let them burn? *Network Security*, 2017(12), 5-9. DOI: 10.1016/S1353-4858(17)30122-8
- Hasan, Md Shamimul, Rashidah Abdul Rahman, Sharifah Farah Hilwani Binti Tengku Abdillah and Normah Omar (2015) Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia, *Journal of Social Sciences*, 11(4): 395.404, DOI: 10.3844/jssp.2015.395.404