BHARATI INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH & DEVELOPMENT (BIJMRD)

(Open Access Peer-Reviewed International Journal)

DOI Link : https://doi.org/10.70798/Bijmrd/04042034

Available Online: www.bijmrd.com | BIJMRD Volume: 4 | Issue: 04(2) | April 2026 | e-ISSN: 2584-1890

Assessment of Awareness of Financial Frauds in the Era of Digital Banking among the Employees

Mr. Libin. R, Dr. Anil Kumar. S. & Dr. Lancy D'Souza

1. 6th Semester (B.A Student), Department of Criminology & Forensic Science, Maharaja's College, University of Mysore, Mysuru, Email: adonai1950s@gamil.com
2. Lecturer, Department of Criminology & Forensic Science, Maharaja's College, University of Mysore, Mysuru.
3. Professor & Head, Department of Psychology, Maharaja's College, University of Mysore, Mysuru.

Abstract: *The advancement of digital banking has significantly transformed financial services by providing speed, convenience, and accessibility. However, this digital transformation has also led to a rise in financial frauds, posing serious challenges to users. The present study aims to assess the level of awareness of financial frauds in the era of digital banking among employees. The study adopts a descriptive research design and collects primary data from employees working in various organizations through a structured questionnaire. The research evaluates employees' awareness of common digital banking frauds such as phishing, online scams, identity theft, fake banking applications, and unauthorized transactions. It also examines their knowledge of preventive measures, cyber-security practices, and responses to fraud incidents. The findings reveal that while employees are generally aware of basic digital banking services, there are notable gaps in their understanding of sophisticated fraud techniques and security protocols. Factors such as educational background, digital literacy, frequency of digital banking usage, and participation in awareness programs significantly influence awareness levels. The study emphasizes the need for regular training sessions, awareness campaigns, and organizational initiatives to educate employees about emerging digital fraud risks. Enhancing awareness among employees is crucial for safeguarding personal and organizational financial assets. The study provides valuable insights for employers, financial institutions, and policymakers to strengthen fraud prevention and promote secure digital banking practices..*

Keywords: *Digital Banking, Financial Frauds, Digital Banking Frauds, Digital Fraud, Policymakers, Fraud Prevention, Secure Digital Banking.*

Introduction: Overview of Financial Frauds in Digital Banking

Rapid technological advancement has transformed the world into a digitally interconnected society where financial activities increasingly occur through virtual platforms. Digital banking has enhanced efficiency, accessibility, and convenience; however, it has simultaneously expanded opportunities for financial fraud. The widespread adoption of mobile banking applications, online payment systems, and fintech services has increased dependency on technology, making individuals and institutions vulnerable to cyber-enabled financial crimes (Vanini et al., 2023).

Employee awareness plays a crucial role in preventing digital financial fraud within banking environments. Bank employees frequently encounter suspicious transactions, phishing attempts, and unusual customer activities. Their vigilance and ability to respond effectively serve as a primary defence against fraud. Developing organizational awareness programs helps institutions maintain regulatory compliance, reduce financial losses, and preserve customer trust (ACFE, 2022).

Digital transactions are preferred due to their speed and convenience. However, increased dependence on online platforms has also exposed users to risks such as phishing links, fake customer support calls, malware attacks, and identity theft. Fraudsters manipulate victims through social engineering techniques, often obtaining confidential banking information within minutes. Applications such as mobile payment platforms and online wallets have unintentionally created new opportunities for cybercriminal exploitation (Ihsan, 2024).

Historically, financial fraud has existed long before digital banking. A notable example is *Irwin and Kerns v. United States (1964)*, a mail fraud case demonstrating that fraud involves not only deliberate deception but also the misuse of trust for unlawful financial gain. Global surveys have also indicated a rising trend in economic crime, with fraud reporting reaching one of its highest levels in recent decades (ACFE, 2022).

Concept of Fraud and Financial Fraud: Fraud refers to intentional deception through concealment, misrepresentation, or omission of facts to obtain unlawful benefits. Contrary to the belief that fraud is victimless, it causes serious financial loss, reputational damage, and psychological distress to victims. At a broader level, fraud increases operational costs for institutions and weakens public confidence in financial systems (Krancher, 2011).

Financial fraud specifically involves deliberate manipulation within financial transactions for personal or organizational gain. According to the Association of Certified Fraud Examiners (ACFE, 2022), such fraud results in economic loss to individuals, corporations, or governments. In India, offences related to cheating and dishonest misappropriation are addressed under legal provisions such as the Indian Penal Code (IPC Sections 420, 403, and 463) and Section 318 of the Bharatiya Nyaya Sanhita (BNS), 2023.

Evolution of Financial Fraud: Financial fraud has evolved alongside economic development. During ancient and medieval periods, fraud commonly involved tax evasion, forged royal documents, counterfeit coinage, and land manipulation. Severe punishments were imposed because cheating the crown was considered betrayal of the kingdom itself.

In the modern era, fraud has become technologically sophisticated. Cybercriminals exploit digital banking systems through phishing, malware, fake investment schemes, cryptocurrency scams, and identity theft. These activities not only cause monetary losses but also damage institutional credibility and economic stability (Ali, 2022).

Digital Banking: Definition and Legal Framework: Digital banking represents the digitization of traditional banking services through electronic channels such as mobile applications, internet banking, automated teller machines, and electronic payment systems. Technologies such as Unified Payments Interface (UPI), digital wallets, and AI-based customer services enable real-time transactions without physical branch visits (Salmony & Harald, 2021).

The Reserve Bank of India (RBI, 2024) emphasizes that digital banking aims to improve transparency, operational efficiency, and financial inclusion. However, cybersecurity threats remain a major challenge. Digital banking operations in India are regulated through multiple legal frameworks including the Information Technology Act, 2000 (Sections 43, 66C, and 66D), the Banking Regulation Act, 1949, RBI guidelines, and criminal provisions under IPC and BNS addressing online cheating and cyber fraud.

Relationship Between Financial Fraud and Digital Banking: Financial fraud and digital banking share an interconnected relationship. While digital banking promotes accessibility and convenience through platforms such as UPI, NEFT, and online transfers, it also increases vulnerability to cyberattacks. Fraudsters exploit fake websites, phishing messages, and social engineering tactics to steal personal information and money. Prevention therefore depends on cybersecurity infrastructure, employee vigilance, and public digital literacy (Nguyen & Huynh, 2021).

Global and Indian Scenario: Historically, fraud evolved from counterfeit trade practices in early societies to Ponzi schemes and stock market manipulation during industrial expansion. The rise of computers and electronic banking in the late twentieth century accelerated digital fraud opportunities. In the twenty-first century, cybercriminals increasingly use ransomware, artificial intelligence, and fake investment platforms targeting global financial systems (Vanini et al., 2023).

In India, banking modernization began during the liberalization period of the 1990s and accelerated with initiatives such as the Pradhan Mantri Jan Dhan Yojana and the introduction of UPI in 2016. These initiatives expanded financial inclusion but also increased exposure to online fraud. Studies indicate a significant rise in banking fraud cases between 2009 and 2021, highlighting the risks associated with rapid digitization (Rao & Agarwal, 2022).

Literature Review: The rapid growth of digital banking has revolutionized global financial systems, yet it has also amplified risks of fraud and cybercrimes. Financial fraud involves deliberate deception for illicit gain, driven not just by technology but by intertwined behavioural, organizational, legal, and criminological elements. Albrecht et al. (2020) frame fraud via the fraud trianglepressure, opportunity, and rationalizationnoting how digital banking's remote access, lax authentication, and staff oversight create fertile ground for asset misappropriation, corruption, and financial statement fraud. They stress fostering ethical cultures, robust internal controls, audits, and forensic tools, while adapting investigations to electronic crimes. Levi and Burrows (2021) describe cyberpiracies crime as a blend of age-old deceit and tech exploitation, critiquing overreliance on tech defences that ignore staff vigilance, leaving doors open to social engineering.

Criminological lenses illuminate employee roles in fraud dynamics. Sutherland's (1949) Differential Association Theory posits crime as learned via social interactions, suggesting workplace norms can normalize deviance, fuelling white-collar offenses among elites. Cohen and Felson's (1979) Routine Activity Theory views crime as converging motivated offenders, suitable targets, and absent guardians; in banks, staff serve as guardians, but poor cyber hygiene erodes this shield, inviting breaches. Gottfredson and Hirschi's (1990) Self-Control Theory links low self-controlimpulsivity and risk appetiteto fraud commission or facilitation, underscoring training to bolster prudent choices.

Global studies reveal fraud's escalating sophistication. PwC's 2022 Global Economic Crime Survey, surveying thousands of firms, found nearly half hit by fraud in two years, with cyber and customer scams topping lists amid digital shifts like online banking and e-commerce. It flags rising supply chain and ESG reporting frauds. Ihsan (2024) spotlights AI-driven threats like deepfakes and scams, showing verification training curbs staff gullibility. Cheng et al. (2024) analyzed Asian banks, linking digital literacy programs to fewer internal frauds and advocating criminologyinfused risk management for resilience.

In India, digitization parallels cyberfraud surges. Rao and Agarwal (2022) document phishing and UPI scams alongside uneven staff readiness, especially in public banks, urging regulatorbacked training. RBI (2023) data for 2022–2023 shows massive losses mostly from human error, not tech flaws, prioritizing vigilance. Singh and Mehta (2021) note theoretical knowledge gaps in spotting phishing or fakes, pushing situational prevention in training.

Behavioural interventions prove potent non-tech shields. Alhassan and Reddy (2021) show cyber hygiene education fosters caution, slashing risks. Veriff's 2025 Global Fraud Index ties AI identity theft spikes to fewer incidents in trained firms, crediting "digital reflexes" from ongoing drills. Kot (2024) dissects affinity fraud, exploiting trust ties, and calls for anti-manipulation education.

Legal knowledge bolsters deterrence. Krancher (2011) pushes updated laws blending penal codes with cyber rules, enhancing sanction awareness. India's Bharatiya Nyaya Sanhita (2023) tackles cheating, impersonation, and trust breaches; the IT Act (2000) hits unauthorized access and fakes, arming staff for reporting.

Tech advances complement but don't supplant human insight. Sawaika et al. (2025) tout AI-federated systems for monitoring, yet insist on human judgment for anomaly spotting. Vanini et al. (2023) attribute most frauds to social engineering over tech fails, recommending resilience training. FATF-Interpol (2023) endorses awareness campaigns, using Routine Activity and Rational Choice theories to shrink opportunities and hike risks via guardianship.

Despite advances in tech, regs, and detection, literature gaps persist. Studies overemphasize tools, sidelining criminological views of staff awareness. Few integrate psychology, law, guardianship, and theory for holistic prevention, especially in Indian banking. Exploring employee awareness, ethics, and criminology intersections is vital for robust defences in digital banking

Methodology: The present study titled "Assessment of Awareness of Financial Frauds in the Era of Digital Banking among Employees" adopted a descriptive research design to examine employees' awareness, perception, and preventive attitudes toward financial frauds within the rapidly evolving digital banking environment. The primary aim was to assess employees' understanding of various digital financial frauds, relevant legal provisions under the Bharatiya Nyaya Sanhita (BNS), Information Technology Act, Indian Penal Code, and related financial regulations, while also identifying sources of knowledge, demographic influences, and perceptions regarding organizational fraud prevention measures. The study involved a sample of 50 employees selected through simple random sampling from different banking and financial institutions, ensuring representation across designations and departments. Data were collected using a structured questionnaire comprising demographic items and Likert-scale statements covering awareness of digital banking frauds, legal provisions, cybercrime and digital arrest scams, institutional preventive practices, and behavioural responses to fraud risks. Responses were obtained through both online and offline survey methods. The questionnaire employed a five-point Likert scale ranging from strongly disagree to strongly agree, allowing systematic quantitative analysis. Descriptive statistical techniques such as frequency, percentage, mean, and standard deviation were used to summarize awareness levels and demographic characteristics, while inferential statistical tools including Chi-square tests and ANOVA examined relationships between demographic variables and fraud awareness. Data analysis was performed using SPSS and Microsoft Excel to ensure accuracy and reliability of findings. The study focused specifically on awareness, perceptions, and preventive preparedness rather than detailed investigation of individual fraud cases or institutional policies. Although limited by a relatively small sample size, geographic scope, short study duration, and reliance on self-reported responses, the research provides valuable insights into existing awareness gaps and emphasizes the importance of continuous employee training, legal literacy, and institutional cybersecurity measures to strengthen fraud prevention practices in the digital banking ecosystem.

Results

Table 1: Distribution of Demographic Details of the Samples

Category	Sub-category	Male	Female	Total respondents	Percentage
Gender	Male	32	-	32	64
	Female	-	18	18	36
Age	25-35	23	14	37	74
	35-45	7	4	11	22
	45 and above	2	-	2	4
Education	Others	4	0	4	8
	Undergraduate	10	3	13	26
	Postgraduate	10	10	20	40
	Professional	8	5	13	26
TOTAL	-	32	18	50	100

The demographic profile of the 50 respondents shows that the majority are male (64%), whereas female respondents account for 36%. Most participants are young adults, with 74% falling in the 25–35 age group, followed by 22% in the 35–45 bracket, and only 4% aged 45 and above. Educational qualification indicates that postgraduate respondents form the largest group at 40%, demonstrating a highly educated sample. Undergraduate and professional qualification holders each make up 26% of the sample, while respondents with other educational backgrounds account for 8%. Overall, the data suggests that the survey was predominantly participated in by young, educated males, which reflects a knowledgeable and aware group of respondents.

Table 2: Distribution of Observed vs Expected Frequency Analysis of Education

Education Level	Observed Male	Observed Female	Total Respondents	Expected Male	Expected Female
Others	4	0	4	2.56	1.44
Undergraduate	10	3	13	8.32	4.68
Postgraduate	10	10	20	12.8	7.2
Professional	8	5	13	8.32	4.68
TOTAL	32	18	50	-	-

The combined table shows both observed and expected frequencies for male and female respondents using digital banking for personal purposes. Out of 50 respondents, 44 people use digital banking, including 27

males and 17 females. Only 6 respondents do not use digital banking, with 5 males and 1 female. The expected values also support this trend, showing approximately 28.16 males and 15.84 females expected to use digital banking, which is very close to the observed values. Similarly, around 3.84 males and 2.16 females were expected not to use digital banking. The Chi-Square p-value is 0.2929, which is greater than 0.05, indicating no significant relationship between gender and the use of digital banking. This means both males and females use digital banking similarly, and the small differences in the numbers occurred naturally without any strong influence. observed values show that out of 50 respondents, 32 were male and 18 were female. Among them, 10 males and 10 females were postgraduates, which is the highest group with a total of 20 respondents. The undergraduate and professional categories each had 13 respondents, where undergraduates included 10 males and 3 females, and professionals included 8 males and 5 females. The "Others" category had 4 respondents, all of whom were male. When compared with expected values, such as 12.8 expected males and 7.2 expected females in postgraduate category, and 8.32 expected males and 4.68 expected females in both undergraduate and professional groups, the differences are small. Since the Chi-Square p-value is 0.177, these variations are not statistically significant, meaning the distribution of males and females across education levels happened normally without any strong pattern.

Table 3: Distribution of Observed vs Expected Frequency Analysis of Age Group

Age group	Observed male	Observed female	Total respondents	Expected male	Expected female
25–35	23	14	37	23.68	13.32
35–45	7	4	11	7.04	3.96
45 & Above	2	0	2	1.28	0.72
TOTAL	**32**	**18**	**50**	**-**	**-**

The observed values show that most respondents belong to the 25–35 age group, with 23 males and 14 females totalling 37 respondents. In the 35–45 category, 7 males and 4 females make up 11 respondents, while only 2 males fall in the 45 and above group. The expected values closely match these counts, such as 23.68 males and 13.32 females expected for ages 25–35, and 7.04 males and 3.96 females for ages 35–45. The Chi-Square p-value of 0.5543 is greater than 0.05, indicating no significant association between age and gender. Therefore, the slight differences between observed and expected values occur naturally, showing that gender distribution across age groups is balanced.

Table 4: Chi-Square Analysis Showing Observed and Expected Frequencies of Digital Banking Usage Across Gender

Particulars	Observed male	Observed female	Total respondents	Expected male	Expected female
Yes	27	17	44	28.16	15.84
No	5	1	6	3.84	2.16
TOTAL	32	18	50	-	-

The combined table shows both observed and expected frequencies for male and female respondents using digital banking for personal purposes. Out of 50 respondents, 44 people use digital banking, including 27 males and 17 females. Only 6 respondents do not use digital banking, with 5 males and 1 female. The

expected values also support this trend, showing approximately 28.16 males and 15.84 females expected to use digital banking, which is very close to the observed values. Similarly, around 3.84 males and 2.16 females were expected not to use digital banking. The Chi-Square p-value is 0.2929, which is greater than 0.05, indicating no significant relationship between gender and the use of digital banking. This means both males and females use digital banking similarly, and the small differences in the numbers occurred naturally without any strong influence.

Table 5: Combined ANOVA Analysis (Education, Age vs Gender)

Factor	Group	Count	Sum	Variance	SS	MS	F	P-Value
Education vs Gender	Male (Column 1)	4	32	8	24.5 (Between)	24.5	1.909	**0.2163**
	Female (Column 2)	4	18	17.67	77 (Within)	12.83	-	-
Education vs Gender	TOTAL	8	50	-	101.5	-	-	-
Age vs Gender	Male (Column 1)	3	46	209.33	60.17 (Between)	60.17	0.460	**0.5346**
	Female (Column 2)	3	27	52	522.67 (Within)	130.67	-	-
Age vs Gender	**TOTAL**	**6**	**73**	**-**	**582.83**	**-**	**-**	**-**

The ANOVA results compare gender differences across education and age categories. For education, males total 32 with an average of 8, while females total 18 with an average of 4.5. The F-value of 1.909 and p-value of 0.216 are both greater than 0.05, indicating no significant difference between males and females in education levels. Similarly, in age analysis, males total 46 with an average of 15.33, and females total 27 with an average of 9. The F-value of 0.460 and p-value of 0.534 again show no significant difference. Therefore, the differences in male and female responses for both education and age groups are due to natural variation, meaning gender does not influence these categories.

Table 6: Percentage Analysis of Digital Banking for personal Use on Male & Female

Particulars	Male	Female	Total repondents	Percentage
YES	27	17	44	**88%**
NO	5	1	6	**12%**
TOTAL	**32**	**18**	**50**	**100%**

The data shows that out of 50 respondents, a large majority of 44 people (88%) use digital banking for personal purposes, while only 6 respondents (12%) do not use it. Among those who use digital banking, 27 are male and 17 are female, showing that both genders actively make use of digital banking services. In comparison, only 5 males and 1 female reported that they do not use digital banking. This indicates that

digital banking is widely accepted and commonly used by most respondents, with only a small number still not preferring or adopting it.

Table 7: Combined Statistical Correlation and t-Test for QST-1, 2, 3 & 4

Particulars	QST 1 (Familiar With Digital Banking)	QST 2 (Regularly Use Digital Banking)	QST 3 (Aware Of Digital Frauds)	QST 4 (Understand How Fraud Occurs)
Strongly Agree	18	23	16	16
Agree	17	11	13	16
Neutral	7	5	15	7
Disagree	3	5	2	5
Strongly Disagree	5	6	4	6
Total Respondents	50	50	50	50

The combined statistical table shows that respondents have a high level of familiarity, usage, and awareness regarding digital banking and digital fraud. For QST1, 18 strongly agree and 17 agree that they are familiar with digital banking, while for QST2, 23 strongly agree and 11 agree that they use it regularly. Only a small number remain neutral (7 and 5) and very few disagree. Similarly, for QST3, 16 strongly agree and 13 agree that they are aware of digital frauds such as phishing and OTP scams, while QST4 shows 16 strongly agree and 16 agree that they understand how fake websites or apps are used for fraud. Neutral responses are higher in QST3 (15) compared to QST4 (7), and disagreement levels are low across both. Overall, all four questions show that the majority of respondents (50 in each question) demonstrate positive knowledge, usage behavior, and awareness of risks in digital banking, indicating strong digital literacy and security consciousness.

Table 8: Combined Statistical Correlation and t-Test for QST 1 VS QST 2 and QST 3 VS QST 4

Statistical Test	QST1 VS QST2	QST3 VS QST4
Mean (Variable 1)	10	10
Mean (Variable 2)	10	10
Variance (Var 1)	49	42.5
Variance (Var 2)	59	30.5
Observations	5	5
Pearson Correlation	0.8416 (Strong Positive)	0.7152 (Strong Positive)
t-Stat	0	0
p-Value (one-tail)	0.5 > 0.05 → Not Significant	0.5 > 0.05 → Not Significant

t Critical (one-tail)	2.1318	2.1318

The correlation and T-test results indicate a strong relationship between the paired questions and show that the differences in responses are statistically insignificant. For QST1 and QST2, both variables have the same mean value of 10, with variances of 49 and 59. The Pearson correlation value of 0.8416 indicates a strong positive relationship, meaning respondents who are familiar with digital banking also tend to use it regularly. The t-statistic is 0 and the p-value is 0.5, which is greater than the significance level of 0.05, indicating that the difference between familiarity and regular usage is not statistically significant. Similarly, for QST3 and QST4, both means remain at 10, with variances of 42.5 and 30.5. The correlation value of 0.7152 shows a strong positive relationship, meaning respondents who are aware of digital frauds also understand how such frauds occur. Again, the t-statistic of 0 and p-value of 0.5 (greater than 0.05) confirm that there is no significant difference between the two variables. Overall, the data shows that respondents demonstrate consistent knowledge, awareness, and understanding of digital banking and digital fraud.

Discussion: The findings emphasize that fraud prevention must extend beyond technical safeguards toward behavioraleducation. Training programs significantly strengthen confidence and preventive engagement. Organizationsshould adopt continuous learning models rather than one-time awareness sessions.Emerging fraud schemes exploit psychological manipulation through fear, urgencyand authority imitation. Digital arrest scams represent a growing concern requiring targeted awareness campaigns.Legal literacy also plays an essential role in strengthening reporting behavior. Employees familiar with relevant legal provisions demonstrate greater willingness to report incidents and seek institutional support also, The findings revealed that majority of the respondents are digitally literate and frequently use online banking platforms such as UPI, mobile banking and internet banking for daily transactions. Data analysis showed strong awareness about digital banking operations and moderate to high awareness about digital financial frauds. For example, 44 out of 50 respondents (88%) regularly use digital banking for personal purposes, indicating widespread acceptance of digital platforms. Chi-square test results, such as $p = 0.5543$ for age vs gender and $p = 0.2929$ for digital usage vs gender, were greater than 0.05, proving that there is no significant association and usage patterns are similar across demographic categories. ANOVA results also showed p-values (0.216 and 0.534) higher than 0.05, concluding that there is no major difference in awareness between male and female respondents and across different qualification groups.

The paired t-tests between familiarity vs regular usage and fraud awareness vs fraud understanding also showed t-stat = 0 and p-value = 0.5, which is greater than 0.05. This means respondents who are familiar with online banking also actively use it, and those aware of frauds also understand how such frauds happen. The strong correlation values of 0.8416 and 0.7152 further confirmed strong positive relationships between the variables. However, the study also identified gaps. Although employees are aware of digital banking, some still lack complete understanding of advanced fraud techniques, cyber laws, and updated legal provisions like BNS. A noticeable portion stayed “Neutral” in questions related to cybercrime awareness, showing the need for stronger training modules and frequent fraud-prevention workshops.

The study proves that employees are largely aware of digital banking and financial fraud, yet continuous training, legal awareness, and updated cybersecurity practices are necessary to strengthen the digital financial ecosystem. The findings highlight the importance of institutional support, periodic workshops, and preventive measures to build a safer and more trustworthy digital banking environment for both customers and banking organizations.

Conclusion: Digital financial fraud awareness represents a critical component of modernorganizational risk management, employees demonstrate familiarity withcommon fraud patterns, emerging threats require continuouseducation efforts.Organizational leadership must prioritize structured training, reporting systems,

andlegal awareness initiatives to strengthen resilience against financial cybercrime.The present study examined the level of awareness regarding financial frauds in the era of digital banking among employees working in banking and financial institutions. The findings indicate that while most employees are familiar with digital banking services and common frauds such as phishing and OTP scams, gaps remain in understanding advanced cyber fraud techniques and updated legal provisions. The rapid growth of digital transactions has increased both convenience and vulnerability, making employee vigilance essential for fraud prevention.The rapid growth of digital transactions has increased both convenience and vulnerability, making employee vigilance essential for fraud prevention. Statistical analysis showed that awareness levels were generally consistent across demographic groups, highlighting the widespread adoption of digital banking practices.

References

- Albrecht, W. S., Albrecht, C., & Zimbelman, M. (2020). Fraud examination (6th ed.). Cengage Learning. www.cengage.ca/c/fraud-examination-6e-albrecht-albrecht-albrecht-zimbelman/9781337619677/?filterBy=Higher-Education
- Alhassan, R., & Reddy, P. (2021). Cyber hygiene and fraud awareness in financial institutions. African Journal of Finance, 18(2), 112–126.www.ijiet.org/vol15/IJIET-V15N2-2235.pdf
- Bharatiya Nyaya Sanhita (BNS), 2023 (India). Government of India Gazette. www.uniexpro.com/2025/11/the-bharatiya-nyaya-sanhita-pdf.html#:~:text=The%20Bharatiya%20Nyaya%20Sanhita%20%28BNS%29%2C%202023%2C%20is%20a,reflect%20modern%20societal%20values%20and%20address%20contemporary%20issues.
- Cheng, D., Liu, J., & Zhao, F. (2024). Risk management and awareness in digital banking: A cross-Asian study. Journal of Risk Management, 32(4), 88–104.https://doi.org/10.1016/j.jclepro.2021.126144
- Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608.http://dx.doi.org/10.2307/2094589
- FATF & Interpol. (2023). Global financial crime trends report 2023. Paris: Financial Action Task Force.www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html
- Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. Stanford University Press.www.psycnet.apa.org/record/1990-97753-000
- Ihsan, M. (2024). The rise of AI-driven financial fraud: Implications for employee awareness. Journal of Financial Crime Studies, 7(1), 54–70.www.scirp.org/reference/referencespapers?referenceid=2244400
- Information Technology Act, 2000 (India). Government of India Gazette.
- Innan, N., Sawaika, A., Dhor, A., Dutta, S., Thota, S., Gokal, H., Patel, N., Khan, M. A.-Z., Theodonis, I., & Bennai, M. (2023).https://doi.org/10.1007/s42484-024-00143-6
- Kot, P. (2024). Affinity fraud and manipulation in digital financial contexts. Journal of Financial Ethics, 12(2), 77–91. www.researchgate.net/publication/378297681_Reviewing_the_role_of_AI_in_fraud_detection_and_prevention_in_financial_services
- Krancher, O. (2011). Financial fraud and penal law: Integrating traditional and digital crime. Indian Law Review, 15(3), 44–60.www.cca.gov.in/sites/files/pdf/ACT/ACT2000.pdf
- Levi, M., & Burrows, J. (2021). The changing contours of financial cybercrime. British Journal of Criminology, 61(5), 1203–1221.www.igi-global.com/chapter/financial-fraud-and-manipulation/364352
- OpenAI. (2025). *ChatGPT (GPT-5.2) [Large language model]*.https://chat.openai.com

- PwC. (2022). Global economic crime and fraud survey 2022. Pricewaterhouse Coopers. www.researchgate.net/publication/303517861_Financial_Fraud_A_Literature_Review
- Rao, K., & Agarwal, S. (2022). Evolution of digital banking and financial fraud in India. Indian Journal of Criminology, 49(2), 33–49.https://doi.org/10.1093/bjc/azn001
- Reserve Bank of India. (2023). Annual report on banking frauds 2022–2023. RBI Publications.
- Sawaika, A., Sharma, R., & Patel, K. (2025). Artificial intelligence and quantum frameworks for fraud prevention. Future Journal of Business & Technology, 14(1), 99–113. www.pwc.com/gx/en/services/forensics/economic-crime-survey/2022.html
- Scholz, R., Czichos, R., Parycek, P., Lampoltshammer, T. J. (2020): Organizational vulnerability of digital threats. A first validation of an assessment method. - European journal of operational research, 282, 2, 627-643.https://publications.rifs-potsdam.de/pubman/item/item_4728904
- Singh, A., & Mehta, R. (2021). Cybercrime in Indian banking: Challenges and prevention. Journal of Economic Crime and Security, 9(3), 65–78.www.researchgate.net/publication/370583841_
- Sorensen, Robert C. (1950). Review of the book *White Collar Crime*, by Edwin H. Sutherland. *American Journal of Sociology, 56*(2), 169–170https://doi.org/10.2307/1138403
- Sutherland, E. H. (1949). White collar crime. Holt, Rinehart & Winston. www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1436
- Vanini, M., Holtz, J., & Keerthi, R. (2023). Social engineering and organizational vulnerability in digital banking. Global Security Review, 11(2), 150–167.https://arxiv.org/abs/2309.01127v1
- Veriff. (2025). Global fraud index report 2025. Veriff Research Division.www.veriff.com/identity-verification/veriff-fraud-index-2025-key-insights-into-the evolving-threat-of-online-fraud
- www.ijrar.orgE-ISSN 2348-1269, P- ISSN 2349-5138

Citation: **Mr. Libin. R, Dr. Anil Kumar. S. & D'Souza. Dr. L.,** (2026) "Assessment of Awareness of Financial Frauds in the Era of Digital Banking among the Employees", *Bharati International Journal of Multidisciplinary Research & Development (BIJMRD)*, Vol-4, Issue-04(2), April-2026.