JOURNAL: PRIMAX INTERNATIONAL JOURNAL OF COMMERCE AND MANAGEMENT RESEARCH
ISSN: Print ISSN: 2321-3604 Online ISSN: 2321-3612, Impact Factor: 7.184
(A DOUBLE-BLIND PEER REVIEWED, OPEN ACCESS REFEREED QUARTERLY JOURNAL)
PRIMAX IJCMR VOLUME NO.12, ISSUE NO-2, JULY -SEPTEMBER - 2024
Research Article

UNDERSTANDING FINANCIAL FRAUD AWARENESS AND CHALLENGES IN KRISHNAGIRI DISTRICT"- A JOURNEY IN THE DIGITAL ERA

Dr.Renuga.R
Assistant Professor, Dept. of Commerce
Government Arts and Science College for Women, Barger
Krishnagiri,-Tamil Nadu

*Corresponding author| Received: 25/07/2024 | Accepted: 20/08/2024 | Published: 08/09/2024

Abstract

Financial Transactions in Our Daily Lives: Embracing Digital Currency and Understanding the Risks of Financial Fraud. In today's world, money transactions play a vital role in our daily lives. Traditional manual handling of cash has been the norm for a long time. However, the current landscape necessitates that almost everyone shifts towards digital transactions. Despite initial hesitancy, people are increasingly embracing digital currency. They now readily transfer even small denominations digitally, and leaving home with a digital wallet has become second nature. In this context, researchers aim to delve deeper into public awareness regarding financial fraud and their experiences with such incidents. Understanding these aspects is essential to help people protect themselves from the increasing frauds in the digital age.

Key words: Digital Currency, Financial Fraud, Public awareness, Digital age

Introduction

The digital era has transformed the way we conduct financial transactions, making it a prevailing aspect of our daily lives. The adoption of digital currency is primarily driven by its significant advantages, including time-saving features, heightened security measures, and unparalleled accessibility. This paradigm shift is profoundly altering the financial landscape, bringing both opportunities and challenges. Initially, obstacles such as the limited availability of smartphones, concerns about accessing digital funds, and apprehensions about handling this new form of currency hindered the widespread acceptance of digital transactions. However, in the current landscape, the installation of digital wallets has become a mandatory and streamlined process, often facilitated by banks. Moreover, numerous private apps have emerged to facilitate effortless money transfers, contributing to the transition to a digital economy. These private apps also offered lucrative offers as part of their acquisition strategy which helped in the quick adoption of digital payment methods. While digital transactions have become commonplace, so have instances of financial fraud. Fraudsters tirelessly work to deceive individuals, irrespective of their educational background. It is against this backdrop that our research endeavours to understand the real-life experiences and awareness levels of the people in Krishnagiri District in Tamilnadu. Our primary objective is to establish a

robust foundation for creating awareness programs and educational initiatives designed to empower individuals to shield themselves from the perils of financial fraud. This study not only seeks to explore the current understanding of financial fraud but also aims to delve into the intricate challenges faced by individuals in Krishnagiri District. By examining these issues, we aspire to promote digital literacy and responsible financial practices, making a significant contribution to the ongoing transition towards a digital economy.

An overview of the term "Financial Frauds"

Financial fraud occurs when someone uses deceptive, misleading, or illegal practices to deprive individuals of their money, assets, or otherwise harm their financial well-being. This can manifest through various methods such as identity theft and investment fraud. To address these issues effectively, it is crucial to report the crimes promptly to the relevant authorities and law enforcement. Additionally, any fraudulent charges should be disputed or cancelled as soon as they are discovered. Victims should also assemble all related documentation, including bank statements, credit reports, and tax forms from current and previous years, and maintain records throughout the reporting process. Regrettably, many victim compensation programs do not cover financial losses resulting from fraud or fraudulent schemes. It is advisable to review your specific state laws regarding victim compensation for clarity. In some cases, seeking legal remedies through civil justice may be the sole option to recover lost funds.

Common Types of Financial Crimes

The below section contains an in-depth overview of common financial crimes

1. Identity Theft:

Identity theft occurs when someone steals your personal financial information, such as credit card numbers, social security numbers, or bank account details, to make fraudulent charges or withdrawals from your accounts. Perpetrators may also use this information to open credit or bank accounts in your name, leaving you responsible for the incurred charges. Identity theft often leads to damaged credit ratings, bounced checks, and being pursued by collections agencies.

2. Investment Fraud:

Investment fraud involves the sale of investments or securities using false, misleading, or fraudulent information. This may encompass false promises, the omission of key facts, insider trading tips, and other deceptive tactics.

3. Mortgage and Lending Fraud:

Mortgage and lending fraud encompass instances where someone opens a mortgage or loan using your information or provides loans with inaccurate information and deceptive practices. This can result in various financial repercussions.

4. Mass Marketing Fraud:

Mass marketing fraud is frequently committed through mass mailings, telephone calls, or spam emails. It commonly involves fake checks, charity scams, sweepstakes, lotteries, and invitations to exclusive clubs or honor societies to steal personal financial information or solicit contributions and fees for fraudulent organizations.

5. Phone Scams:

These may involve phone calls claiming to be from government agencies, banks, or other "official" entities, often with the intent to defraud individuals.

Reporting of Financial Fraud in India

In India, one can report financial frauds to the following authorities and organizations:

1. Local Police: Start by filing a First Information Report (FIR) with your local police station. Provide them with all the necessary details and evidence related to the financial fraud.

2. Reserve Bank of India (RBI): If the fraud is related to a banking or financial institution, you can report it to the RBI. They regulate and oversee banks and financial institutions in India.

3. Securities and Exchange Board of India (SEBI): If the fraud involves securities or investment-related matters, such as stock market fraud or fraudulent investment schemes, you should report it to SEBI. They are the regulatory body for the securities and commodities market in India.

4. Economic Offenses Wing (EOW): In some states in India, there is a specialized wing known as the Economic Offenses Wing that handles financial frauds. One can approach state's EOW for assistance.

5. Central Bureau of Investigation (CBI): For more serious and complex financial fraud cases, one can contact the CBI, which is India's premier investigative agency.

6. Cyber Crime Cell: If the financial fraud involves online or cyber-related activities, one can report it to your state's Cyber Crime Cell. They handle cybercrimes, including online financial frauds.

7. National Consumer Helpline: One can contact the National Consumer Helpline at 1800-11-4000 or 14404 (toll-free) to report consumer-related financial frauds and seek guidance.

8. Banking Ombudsman: If the fraud is related to a bank and if one aisre unable to resolve the issue with the bank, they can approach the Banking Ombudsman. Each bank has its own Ombudsman, and details are available on the RBI's website.

9. State Consumer Disputes Redressal Commission: If the fraud is consumer-related, one can file a complaint with their State Consumer Disputes Redressal Commission. Each state has its own commission.

10. Local Consumer Forum: One can also approach your local Consumer Forum for resolution of consumer-related financial frauds.

It's important to provide as much information and evidence as possible when reporting a financial fraud to any of these authorities or organizations. Additionally, one may consider seeking legal advice to guide through the reporting and resolution process.

Background of the study

Financial transactions are an integral part of daily life, with the traditional handling of cash gradually giving way to digital currency in today's digital era. The shift towards digital transactions has been driven by the convenience, security, and accessibility offered by digital currency, prompting more individuals to embrace this form of monetary exchange. However, alongside the increasing adoption of digital currency comes the heightened risk of financial fraud. Despite the growing acceptance of digital transactions, individuals remain vulnerable to various forms of financial fraud, including identity theft, investment fraud, and mass marketing fraud. In Krishnagiri District, as in many other regions, there exists a need to comprehensively understand the awareness levels and real-life experiences of individuals regarding financial fraud. This understanding is crucial for empowering individuals to protect themselves against fraudulent activities and safeguard their financial well-being in the digital age. Against this backdrop, researchers aim to delve deeper into public awareness regarding financial fraud and their experiences with such incidents specifically within Krishnagiri District. By conducting this study, researchers seek to identify the challenges faced by individuals in the district concerning financial fraud and to promote digital literacy and responsible financial practices. The ultimate goal of this research is to establish a robust foundation for creating awareness programs and educational initiatives tailored to the needs of the community in Krishnagiri District. Through these efforts, the study aims to contribute

to the ongoing transition towards a digital economy while mitigating the risks associated with financial fraud for individuals in the region.

Merits of the Digital Financial Landscape with Regard to Understanding Financial Frauds

Digital financial transactions offer unparalleled convenience, allowing individuals to conduct transactions anytime and anywhere with internet access. Digital transactions eliminate the need for physical visits to banks or other financial institutions, saving time for both consumers and businesses. The widespread availability of smartphones and internet connectivity has made digital financial services accessible to a broader segment of the population, including those in remote areas. Many digital payment platforms employ advanced security measures such as encryption and multi-factor authentication to safeguard transactions and protect against fraud. Digital financial transactions streamline processes and reduce paperwork, leading to increased efficiency in financial operations for both individuals *and businesses.*

Demerits of the Digital Financial Landscape with Regard to Understanding Financial Frauds

The digitization of financial transactions has also led to an increase in cybercrimes and financial fraud, as fraudsters exploit vulnerabilities in digital systems to deceive individuals and organizations. The complexity of digital financial systems and the variety of digital payment methods available can be overwhelming for some users, leading to confusion and potentially increasing the risk of falling victim to fraud. Relying solely on digital financial transactions makes individuals and businesses vulnerable to disruptions caused by technical glitches, cyber-attacks, or system failures. Digital financial transactions often involve the collection and sharing of personal and financial data, raising concerns about privacy and data security among users. Despite efforts to enhance accessibility, certain marginalized or vulnerable groups may still face barriers to accessing digital financial services, exacerbating inequalities in financial inclusion.

Overall, while the digital financial landscape offers numerous benefits, it is essential for users to be aware of the associated risks and take proactive measures to protect themselves against financial fraud and cybercrimes. Education, awareness programs, and robust security measures are crucial for fostering a safe and secure digital financial environment for all users.

The Digital Financial Landscape and Understanding Financial Frauds in Krishnagiri District, Tamil Nadu, India

Krishnagiri district, situated in the north western part of the state of Tamil Nadu, India, holds significant importance both geographically and economically. Known for its agricultural productivity, the district boasts a diverse economy comprising agriculture, manufacturing, and services sectors. With a population that is increasingly embracing digitalization, Krishnagiri district serves as an interesting case study for understanding the digital financial landscape and its implications for mitigating financial frauds.

The advent of digital financial services has reshaped the way financial transactions are conducted in Krishnagiri district. The district has witnessed a rapid proliferation of digital payment platforms, mobile banking services, and electronic fund transfers. This digital transformation has been fuelled by several factors, including government initiatives to promote financial inclusion, improvements in internet connectivity, and the widespread adoption of smartphones.

Amidst the transition towards digital financial transactions, understanding financial frauds has become paramount in Krishnagiri district. As individuals and businesses increasingly rely on digital platforms for financial transactions, they are exposed to various forms of financial fraud, including identity theft, online scams, and phishing attacks. The prevalence of financial frauds poses significant risks to the financial well-being of individuals and undermines trust in digital financial systems.

In this context, efforts to enhance understanding of financial frauds in Krishnagiri district are crucial for fostering a secure digital financial landscape. Awareness campaigns, educational initiatives, and capacity-building programs play a vital role in empowering individuals to recognize and mitigate the risks associated with financial frauds. Furthermore, collaboration between government agencies, financial institutions, and civil society organizations is essential for developing comprehensive strategies to combat financial frauds effectively.

Moreover, given the district's agricultural heritage and diverse economic activities, tailored interventions are needed to address the unique challenges and vulnerabilities faced by different segments of the population. For instance, farmers and rural residents may require specific guidance on safeguarding their financial assets in the digital realm, while small businesses may benefit from training programs on cyber security best practices.

Krishnagiri district stands at the intersection of digital innovation and financial resilience, presenting both opportunities and challenges in the realm of digital finance. By leveraging its

economic strengths and embracing digital technologies responsibly, the district can chart a path towards inclusive and sustainable growth while safeguarding against financial frauds in the digital age.

Review of Literature

Chandra, Akhilesh, and Melissa J. Snowe (2020) introduces a theory-based taxonomy for cybercrime is developed to address the lack of clear definitions and standards in measuring and managing cybercrime. Cybercrime is defined as any criminal activity utilizing computer technology. The taxonomy comprises four key elements: mutual exclusivity, structure, exhaustiveness, and well-defined categories, forming the theoretical framework. Exemplars and heuristics are employed to validate the taxonomy as a proof-of-concept. The contributions of the taxonomy to both theoretical understanding and practical application are outlined, with discussions on its implications for management, reporting, disclosure, governance, regulation, and judicial processes.

Abdul Rehman (2021) highlights the increasing prominence of cybercrime targeting or utilizing computer networks, with particular emphasis on the IoT domain. Despite challenges, digital forensics plays a crucial role in securing IoT environments. The escalation of privacy and security concerns in digital forensics underscores the need for focused attention on privacy issues alongside security measures. Rehman notes a significant gap in addressing privacy concerns compared to security in cybercrime discussions. The article proposes a classification matrix and a system to mitigate privacy threats and attacks, aiming to address this gap and contribute to the field of cyber security.

Saldaña-Taboada (2022) highlights the phenomenon of "offending concentration" in traditional offline crime, where a small proportion of offenders is responsible for a large proportion of crimes. However, there's limited research on this concentration in cybercrime. The study focuses on victim reports of Bitcoin-related cybercrimes to examine the extent of offending concentration and identify groups of online offenders. Results show that a significant number of cybercrimes are linked to a small number of highly active Bitcoin addresses, but not necessarily those yielding the highest financial gains.

Kim (2023) emphasizes the global rise of cybercrime and the lack of effective measures to combat it, necessitating an analysis of cybercriminal behavior. Through classification into three types—integrity-related, computer-related, and content-related—this study identifies key factors driving each type of cybercrime and proposes measures to counteract them. By interviewing specialized police officers, the study derives main crime factors from the

perspective of offenders, contributing to the literature on cybercrime and offering preventive measures tailored to each type.

Dr. Leena B. Dam and Kalyani Deshpande (2020) state that general users of e-banking are not completely aware of the risks involved in digital banking. Even users with a good educational background get deceived in digital scams. (Deshpande, 2020)

Curtis (2023) discusses the increasing prominence of cybercrime, particularly within the Internet of Things (IoT) domain, and highlights challenges in digital forensics. While security concerns have received considerable attention, the article underscores the growing importance of privacy in cyber security, especially in combating cybercrime. The study proposes a classification matrix and a system to address privacy threats and attacks in digital forensics, aiming to fill a gap in research on privacy challenges in cyber security against cybercrime.

Research Gap

The existing research primarily focuses on cybercrime in IoT environments and provides theoretical insights into its nature. However, there is a notable gap in understanding the practical implications of cybercrime, particularly its impact on financial frauds, which are crucial for the development of all districts in India. This research gap highlights the need for empirical studies to explore the real-world consequences of cybercrime on financial frauds, informing policy decisions necessary for the holistic development of all districts in India.

Objective

To study the awarness levels of financial frauds in Krishnagiri district.

Research Design

The research aims to gauge the current awareness levels regarding financial fraud cybercrime in Krishnagiri district, Tamil Nadu, India. Utilizing a combination of primary and secondary data, secondary sources such as bank websites, research journals, and online newspapers were consulted. Primary data was gathered through a structured questionnaire distributed to respondents in Krishnagiri.

Research Methodology

The study draws upon both primary and secondary data sources. Secondary data informed the formulation of questionnaires, while primary data serves as the cornerstone of the research.

Area covered from Primary Data

The research was conducted in Krishnagiri district, Tamil Nadu, renowned for its rapid development within the state. Situated in close proximity to Bangalore city, Karnataka,

Krishnagiri has seen a surge in industrial growth with the establishment of major companies such as Delta, Tata, and OLA. This influx of industries has led to increased employment opportunities, resulting in a significant rise in digital transactions.

Importance of the study

The historical significance of Krishnagiri district, along with its proximity to Bangalore, Karnataka, has been instrumental in its economic growth. With a rich history dating back to ancient times, Krishnagiri has served as a hub for trade and commerce, attracting various civilizations to its region. The establishment of major industries like Delta, Tata, and OLA near Bangalore has provided abundant employment opportunities, fuelling economic progress and facilitating digital transactions. Despite this advancement, understanding the intricacies of financial fraud in digital transactions remains crucial. Identifying the major challenges faced during digital transactions is imperative for society to provide safeguards and ensure secure transactions for all individuals.

Analysis and Interpretation

Demographic details

Table : 1 : Socio- Economic Characteristics

Personal Details of the Respondent		Frequency	%
Gender	Male	39	29.5
	Female	93	70.5
Age in years	21-30	47	35.6
	31-40	47	35.6
	41-50	22	16.7
	51-60	16	12.1
Educational Qualification	Up to School Level	19	14.4
	Under Graduate	34	25.8
	Post Graduate	45	34.1
	Others	34	25.8
Occupation	Self-Employed	36	27.3
	Private-Employee	59	44.7
	Government employee	23	17.4
	Professionals	14	10.6
Monthly Income	Below 20000	62	47.0
	20001-30000	21	15.9
	30001-40000	19	14.4
	40000-50000	14	10.6
	50000-60000	7	5.3
	60000-70000	3	2.3
	70000-80000	2	1.5
	Above 80000	4	3.0
Total		132	100

Source: Primary data

The data shows that the majority of respondents were female, accounting for 70.5% of the total, while males constituted 29.5%. Regarding age distribution, respondents were fairly evenly spread across different age groups, with the highest proportions in the 21-30 and 31-40 brackets, each comprising 35.6% of the total. In terms of educational qualifications, the largest proportion held postgraduate degrees (34.1%), followed by undergraduate qualifications (25.8%), while a significant portion had educational qualifications up to the school level (14.4%). Occupationally, the majority were private employees (44.7%), followed by self-employed individuals (27.3%) and government employees (17.4%), with professionals comprising the smallest proportion (10.6%). Regarding monthly income, the highest number of respondents reported earnings below 20,000 rupees (47.0%), followed by those earning between 20,001 and 30,000 rupees (15.9%), with fewer respondents reporting higher income brackets, including only 3% earning above 80,000 rupees per month. Overall, the data reflects a diverse sample in terms of gender, age, educational background, occupation, and income level, providing a comprehensive overview of the respondents' demographics.

Impact Factors on awareness of financial Frauds

Data Reliability

Table 2: Reliability Statistics

Cronbach's Alpha	N of Items
.869	17

Reliability: A Cronbach's Alpha of 0.869 is generally considered to be a good level of reliability. It indicates that the 17 items in your questionnaire or scale are reasonably consistent in measuring the same underlying construct. This suggests that the items are reliable in capturing the concept one intends to measure.

Table 3: Factor Analysis-KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.802
Bartlett's Test of Sphericity	Approx. Chi-Square	363.674
	Df	28
	Sig.	.000

Source: Computed

Based on the KMO value and the low p-value from Bartlett's Test of Sphericity, it appears that the data is suitable for factor analysis. These results suggest that there is a good level of sampling adequacy, and the correlations between variables are statistically significant, which supports the use of factor analysis or related techniques to explore the underlying structure of data set.

Table 4: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.972	62.154	62.154	4.972	62.154	62.154	3.458	43.220	43.220
2	1.131	14.141	76.295	1.131	14.141	76.295	2.646	33.074	76.295
3	.598	7.474	83.769						
4	.365	4.568	88.337						
5	.308	3.855	92.192						
6	.279	3.485	95.677						
7	.239	2.984	98.661						
8	.107	1.339	100.000						

Extraction Method: Principal Component Analysis.

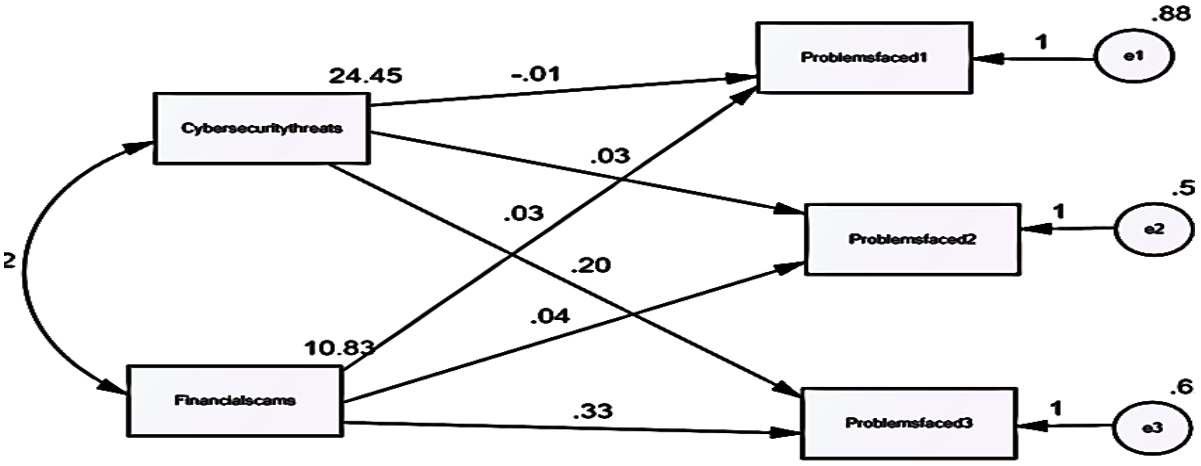
Table 5 :Rotated Component Matrix

Awareness about	Component	
	1	2
Risky app downloads.	0.842	
Pin capture through cameras.	0.81	
Financial credential theft via screen sharing apps.	0.792	
Social media medical scam.	0.821	
Job and shopping portal scams.	0.719	
Deceptive link downloads.		0.832
Lottery scam.		0.921
Deceptive loan ads.		0.75

Table 5 explains the rotated component matrix is a way to understand how different variables are related to underlying factors or components. Component 1 appears to be associated with “Cyber security threats”, while Component 2 appears to be associated with “Financial scams”. The loadings indicate the strength of the relationship between each variable and the component. Higher loadings indicate a stronger association with that component.

Structural Equation Modelling

SEM utilizes various statistical techniques, such as confirmatory factor analysis (CFA) to assess the measurement model's fit to the data and structural equation modeling to estimate and test the relationships specified in the structural model. SEM is a powerful tool for testing complex theoretical models and examining the underlying structures of relationships among variables in social science research.



Problem Faced 1 – named as “Financial Scams”

Problem Faced 2- named as “Phone Scams”

Problem Faced 3 – named as “Phishing Scams”

Table: 6 Model Fit

Model	CMIN/DF	P-Value	GFI	AGFI	CFI	RMSEA
Recommended Value	1 to 5	Less than 0.05	Greater than 0.9	Greater than 0.9	Greater than 0.9	Less than 0.08
Output value	1.633	0	0.969	0.845	0.988	0.009

The model suggests that knowledge about digital financial scams:

1. Empowers individuals to confront real issues stemming from these scams.
2. Enhances preparedness in dealing with the challenges posed by such scams.
3. Provides a crucial defence against the adverse effects of digital financial fraud.
4. Equips people with the tools to respond effectively to the problems caused by these scams

Findings of the study

The findings from the rotated component matrix suggest that the data can be organized into two distinct components: "Cyber security threats" and "Financial scams". Component 1, labelled as "Cyber security threats", encompasses variables related to cyber security threats, while Component 2, labelled as "Financial scams", comprises variables associated with financial frauds.

The model implies that knowledge about digital financial scams plays a crucial role in several aspects:

1. Empowerment: Understanding digital financial scams empowers individuals to confront real issues arising from these scams.

2. Preparedness: Knowledge about financial scams enhances preparedness in dealing with the

challenges posed by such fraudulent activities.

3. Defence: It provides a crucial defence against the adverse effects of digital financial fraud by enabling individuals to recognize and mitigate potential risks.

4. Response: Having knowledge about digital financial scams equips people with the necessary tools to respond effectively to the problems caused by these scams, thereby minimizing their impact.

Overall, the findings highlight the importance of awareness and education in combating digital financial scams and emphasize the role of knowledge in protecting individuals from falling victim to fraudulent activities in the digital realm.

Conclusion and Recommendations

The study sheds light on the evolving landscape of financial transactions and the growing acceptance of digital currency in our daily lives. It is evident that the transition towards digital financial practices brings both opportunities and challenges.

In the Krishnagiri District, as in many places, the initial reluctance towards digital transactions has given way to widespread adoption, driven by the ease of use and accessibility. However, this transition has also exposed individuals to various financial fraud risks.

The study recognizes that individuals in Krishnagiri District, like many others, have encountered financial fraud incidents, indicating the need for increased awareness and preparedness. The research serves as a valuable foundation for creating educational initiatives and awareness programs to empower individuals to protect themselves in this digital age.

The study acknowledges the importance of understanding financial fraud, including its various forms such as cyber threats, phone scams, and phishing scams. By examining these issues, the research contributes to promoting digital literacy and responsible financial practices, ultimately aiding the ongoing transition towards a digital economy.

Additionally, the study emphasizes the significance of promptly reporting financial fraud to the relevant authorities and organizations in India, which play a pivotal role in addressing and mitigating financial fraud-related issues.

In conclusion, this research not only highlights the prevalence of digital financial scams but also underlines the need for robust education and awareness programs to equip individuals with the knowledge and tools to safeguard themselves in the digital era. It further underscores the importance of effective reporting mechanisms to address financial fraud, contributing to a safer and more secure financial environment for all.

References

- https://www.infosecawareness.in/concept/guidelines-to-report-financial-frauds-in-india?lang=en
- https://www.hindustantimes.com/business/financial-fraud-top-cyber-crime-in-india-upi-e-banking-most-targeted-study-101695036325725.html
- https://www.researchgate.net/publication/356887995_Financial_Cybercrime_A_Comprehensive_Survey_of_Deep_Learning_Approaches_to_Tackle_the_Evolving_Financial_Crime_Landscape
- https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20final.pdf
- **Chandra, Akhilesh, and Melissa J. Snowe.**"A taxonomy of cybercrime: Theory and design." *International Journal of Accounting Information Systems* 38 (2020): 1004676.
- **Aziz, Omer, M. Abdullah Siraj, and Abdul Rehman**. "Privacy challenges in cyber security against cybercrime in digital forensic. A systematic literature review in Pakistan." *Journal of* Computing *& Biomedical Informatics* 2.02 (2021): 158-164.
- https://www.researchgate.net/publication/356167874_Offending_Concentration_on_the_Internet_An_Exploratory_Analysis_of_Bitcoin-related_Cybercrime